Lenovo

LDI Plus User Guide

Copyright/Disclaimer

This document contains proprietary information of Lenovo that is protected by copyright and other intellectual property law which restricts its usage. The content in this document is subject to change without notice. If you find any issues in the documentation, please report to us in writing. Lenovo gives no representations or warranties of any kind regarding its content, including accuracy or completeness. Please do not reproduce or transmit any part of this document in any form or by any means, electronic or mechanical, for any purpose, without a written approval from Lenovo.

Revision History

Version	Published On	Description
1	24 March 2022	A consolidated User Guide comprising all other guides in it.
2	14 April 2022	Updated for 2.14 release
3	10 June 2022	Updated for ServiceNow Integration, Customer Facing Troubleshooting, etc.
4	8 August 2022	Updated with Ivanti Endpoint Manager Guide
5	25 August 2022	Updated for 2.18 release, notably revised to include new device status.
6	29 September 2022	Updated for 2.19 release, notable revised to include new Action Builder tool in Automations section.
7	8 December 2022	Updated for 2.21 release, notably revised network port requirements.
8	10 February 2023	Updated for 23.02 release, notably with improved uninstallation options and Manage Dashboards feature.
9	26 April 2023	Updated for 23.04 release, notably with Import Labels feature, Manage Dashboards improvements, and ability to subscribe to status page within portal (https://ldiplusstatus.uds.lenovo.com).
10	3 June 2023	Updated for 23.05 release, notably with Linux support, daily report processing (instead of weekly), permissions consistency, Executive Insights dashboard, and speed improvements.
11	9/13/2023	Updated to include battery replacement or repair info and improved JAMF instructions.

Contents

1 Overview

Lenovo Device Intelligence Plus (LDI Plus) is an enhanced predictive and proactive SaaS tool for the smarter PC fleet management. Lenovo Device Intelligence Plus gives enterprise IT Administrators advanced predictive insights to help pinpoint hardware and systemic issues before they occur.

Delivering in-depth device and business insights, the LDI Plus solution is an AI-powered SaaS PC health management tool. The solution identifies critical issues across the fleet, both current and potential, monitors for hardware failures, Blues Screen of Death (BSODs), and system and software applications causing performance degradation. For the organization requiring smarter insights into PC health, LDI Plus features a deeper level of analytics such as persona analysis, digital user experience scoring, asset optimization, productivity impact assessments, root cause analysis, sector benchmark comparisons, remediate issues, and more. This enables customers to monitor, analyse, predict, prevent, and optimize their IT environments for better business outcomes.

1.1 Use cases

LDI Plus software through its predictive analytics of device functioning and issue detection capability helps the organization to:

- Reduce support calls
- Reduce breakdowns and increase device uptime and productivity
- Improve customer experience

An IT Manager, Analyst, or Administrator can use this tool to predict, detect, and resolve issues before they negatively impact employees' productivity.

Features and tools are available to address use cases in LDI Plus. For more details, refer to LDI Test Drive.

1.2 Features and Licenses

LDI Plus enables you to proactively support the system users through AI and ML techniques to predict the failures that might occur in users' devices.

Besides, you can monitor device performance in real-time, detect, and report the issues when they occur.

LDI Plus also provides:

- Options to execute issue fixes
- Root cause and correlation analysis capabilities
- Application comparative and trend analytics
- Assessment of IT's impact on employee productivity
- Digital UX scoring to quantify end-user experience with their IT resources
- External and internal data benchmarking
- Employee workstyle personas mapped to IT resources

- Asset optimization analytics to help size hardware and software investments

1.3 Get Help When Using Tool

This chapter provides you valuable information about how to put the product to use.

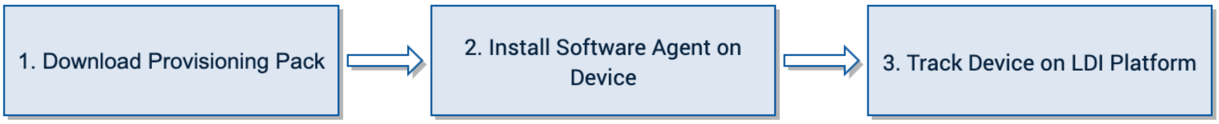
You can reach out to LDI Plus support in multiple ways to get help if you face any issues in using the tool:

- Report the problem to the support team. Send an email to ldisupport@lenovo.com.
- Report the problem in the interface. Refer to Raise a Ticket.

2 Onboard Your Fleet

2.1 Onboard Your Fleet

This chapter helps you smoothly onboard the fleet of devices in your organization to the LDI platform.


1. Download Provisioning Pack
2. Install Software Agent on Device
3. Track Device on LDI Platform

This can be installed by running the executable on individual devices or by using an endpoint management utility such as SCCM, Microsoft InTune, or Ivanti that have been tested and approved for LDI deployment. Other endpoint management utilities will likely work as well.

2.1.1 Software Requirements

Client software for this solution has a few requirements that the device must meet.

Category	**Requirement**
Manufacturer	Any device manufacturer is supported, though some features may only be available on the Lenovo devices.
Operating System	Windows: • Windows 10: 64 bit version 1809 (October 2018 Update) or newer • Windows 11: 64-bit • Windows 10S or 10x editions are not supported. • VMs are supported using alternate installer macOS: • macOS versions 10.9 and above are supported. • Intel and Apple Silicon CPUs are supported. Linux: • Red Hat Enterprise Linux version 7 and 8 • Amazon Linux version 2 • CentOS Version 7 or later • Fedora Version 35 • Oracle Linux Version 7 or later • SuSE Enterprise Linux version 12 or later • openSuSE Leap version 15.3 • Ubuntu version 14, 18 or later • Debian version 10 or later • Mageia version 8 • Mint version 19, 20.2 or later

Category	Requirement
Hardware	• Trusted Platform Module (TPM) 2.0 enabled • Processor supports x86 instruction set architecture
Environment	• Access to the Internet - *.uds.lenovo.com on port 443 (include port 8883 if UDC agent older than 22.10.0.5) and *.lakesidesoftware.com on port 443 • **Proxy is supported in some scenarios**. Devices may require additional configuration to support.
Proxy Support	You must configure the proxy through WinINet (WinHTTP or a third-party application/browser extension). • Proxy server can reach *.uds.Lenovo.com on port 443 (include port 8883 if UDC agent older than 22.10.0.5) and *.lakesidesoftware.com on port 443 DNS name resolution is available on each managed device. You cannot set an authentication on the proxy server.

2.1.2 Download Provisioning Package

You can onboard fleet of devices to LDI platform through:

- Instructions and Agents (Preferred)
- Devices page (optional)

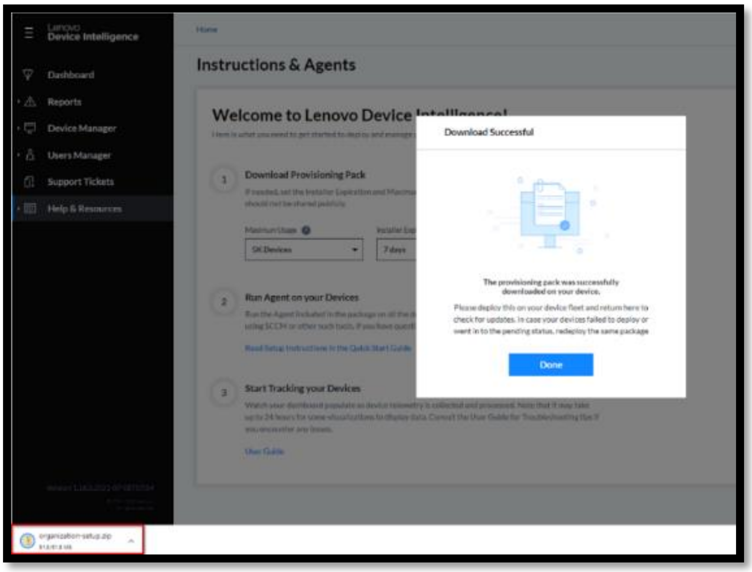
1. Click **Help & Resources** and then click **Instructions & Agents**. The **Instructions & Agents** page appears.

- Select **Windows (Physical)** to onboard a physical device. For further details, refer to Install a Physical Device.
- Select **Windows (Virtual)** to onboard a virtual machine. For further details, refer Install the Agent to a Virtual Machine.
- Select **macOS** to onboard a macOS device. For further details, refer to Install a macOS Device.

- Select **Linux** to onboard a Linux device. For further details, refer to Install a Linux Device.

2.1.3 Install a Physical Device

1. Follow the instructions in Download Provisioning Package.
2. Click **Confirm**.
3. In the **Maximum Usage** drop-down list, select the number of devices on which you can download the provisioning package.
4. In the **Installer Expiration** drop-down list, select the days for which the provisioning pack installation is valid.
5. Click **Download Pack**. The pack is downloaded on the device, which access the portal.



Download Successful

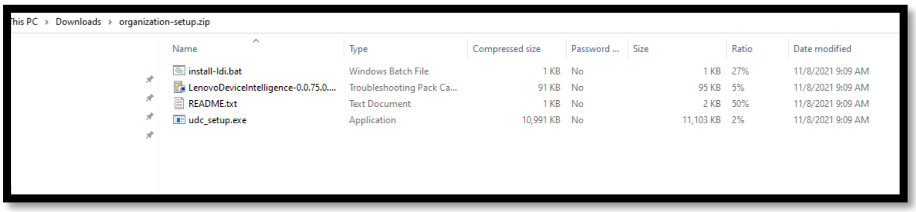
The provisioning pack was successfully downloaded on your device.

Please deploy this on your device fleet and return here to check for updates. In case your devices failed to deploy or went in to the pending status, redeploy the same package

The package, organization-setup.zip which has the following components:

- **install-ldi.bat** - A script that has series of commands for installation for LDI software.

1. A Windows-based troubleshooting file package, **LenovoDeviceIntelligence-0.0.75.0.diagcab**. To know more about how to install, run, and create the LenovoDeviceIntelligence.diagcab file, refer to Troubleshooting.
2. README.txt file
3. **udc_setup.exe** - UDC setup, UDC Service information, and task control settings



This PC > Downloads > organization-setup.zip

Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
install-ldi.bat	Windows Batch File	1 KB	No	1 KB	27%	11/8/2021 9:09 AM
LenovoDeviceIntelligence-0.0.75.0....	Troubleshooting Pack Ca...	91 KB	No	95 KB	5%	11/8/2021 9:09 AM
README.txt	Text Document	1 KB	No	2 KB	50%	11/8/2021 9:09 AM
udc_setup.exe	Application	10,991 KB	No	11,103 KB	2%	11/8/2021 9:09 AM

2.1.4 Install Software Agent on Device

Note: The setup is unique for the organization and must not be shared.

Execute the following steps on every device in the fleet.

1. Copy the following files to an empty folder in the device, e.g., C:\temp\LDItemp
   - udc_setup.exe
   - README.txt
   - install-ldi.bat
2. Execute the batch file as an Administrator.
   - Open the command prompt as an Administrator
   - Execute cd C:\temp\LDItemp
   - .\install-ldi.bat
3. Confirm whether device onboarding was successful or not by checking for an error in the registry.

UDC records the error in the Windows Registry at HKLM\SOFTWARE\LENOVO\UDC\CriticalTranscript when onboarding fails.

If there is an error during installation, check the following error code table to identify the error and rectify it by following the remedial tips:

UDC Significant Event Codes	Error Name	Remedial Tip
None	Ok	
1016:12007	PortalUnreachable	Ensure you have a proper network connectivity and check the connection to the UDS portal.
1001:80	CertificateMismatch	Portal certificate is not valid. Check for https proxy (like Fiddler) that overrides server certificate. Otherwise, contact Lenovo, because server certificate could have been changed.
1001:85	TokenExpired	LDI portal token has expired, or the device registration limit set for this token is over. Request for a new provisioning package with a new token.
1001:86	TokenNotValidated	UDS does not accept provided token. Create another provision package or contact the administrator.

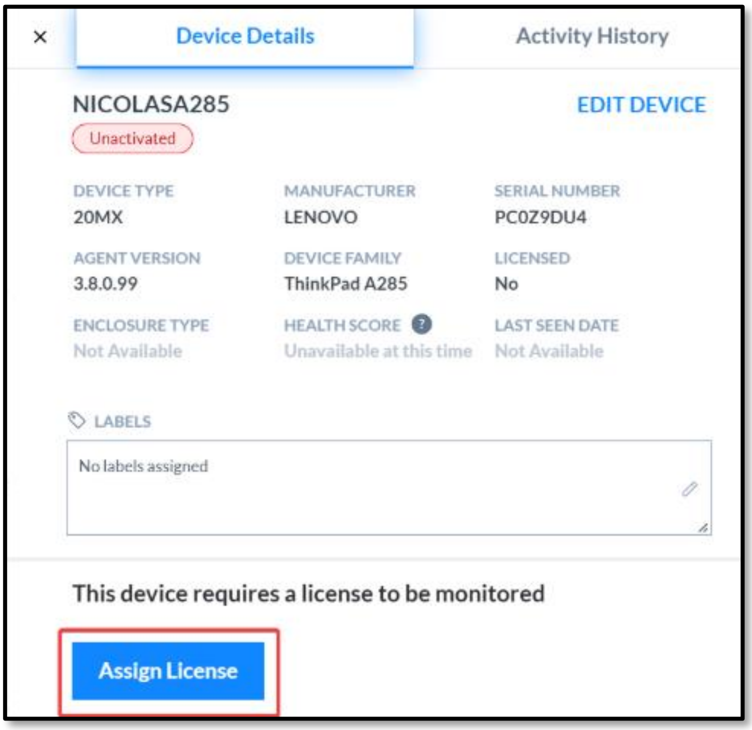
1016	RegisteredToAutomaticOrg	The device was registered to an automatic organization. Restart UDCService and log in again. If it fails, contact the administrator.
	DeviceAlreadyRegistered	This device was already registered in the portal. No other action may be needed, but we recommend you follow the uninstallation steps including deletion from the portal before attempting to reinstall and register the device to the portal. Refer to Uninstall UDC.
1016	UnableToRetrieveClaimCode	The script /UDC was unable to retrieve the activation code required for registration of the device in the portal. Restart UDCService and try again. If it fails, contact the administrator. To restart the UDC Service, follow these options: Press Windows + R → Enter services.msc → Select UDC Client Service → Restart Restart the device and log in to the LDI Plus portal again.
1011	RegistrationTo Organization Failed	device_path in the C:\ProgramData\Lenovo\Udc\Shared\ConfigPolicy.json.signed is empty or this file is missing. Check for the UDC Error and UDC log files. **Note**: Check for the log files in C:\ProgramData\Lenovo\Udc\Log ConfigAgent log file informs you if the config policy has been updated from UDS DeployAgent log file informs you if the package has been installed successfully. Navigate to C:\ProgramData\Lenovo\Udc\Download to see the Provisioning Package ID.

2.1.5 Track Device on LDI

1. Check the **Devices** page to track whether the device has been onboarded to the LDI or not.
2. Check the device status. If the status is:
   - **Pending** - The device could not be onboarded because of an error. Check for the type of error code in the registry and follow the remedy tip provided for it in the error code table. This also includes devices that don’t have an assigned license.
   - **Active** – Device has successfully onboarded and is currently online.
   - **Offline** - Device has successfully onboarded and is currently offline.

Note: To get a license, follow these steps:

1. Select Device Manager → Devices.
2. Search for the device with ‘Unassigned License’



NICOLASA285
Unactivated

DEVICE TYPE: 20MX
MANUFACTURER: LENOVO
SERIAL NUMBER: PC0Z9DU4
AGENT VERSION: 3.8.0.99
DEVICE FAMILY: ThinkPad A285
LICENSED: No
ENCLOSURE TYPE: Not Available
HEALTH SCORE: Unavailable at this time
LAST SEEN DATE: Not Available

No labels assigned

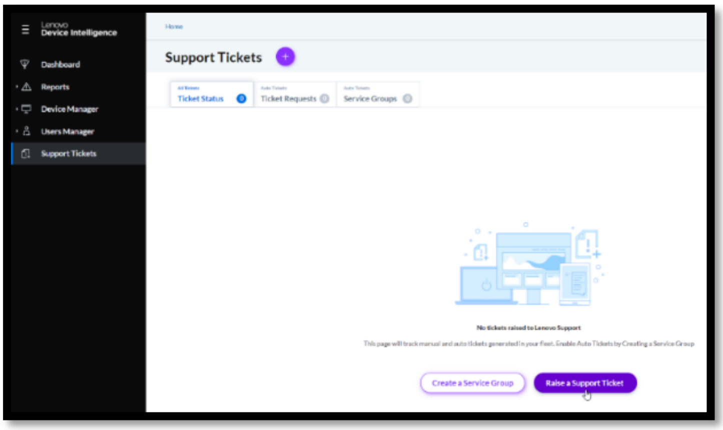
This device requires a license to be monitored

3. Click Assign License.

- **Offline** - Devices that do not send data to the system for 5 minutes. These devices are moved from Active Status to Offline Status. If the device does not have a license, it becomes Unactivated with Pending status.

2.1.6 Raise a Ticket

Raise a ticket if the error persists even after following the remedial tip from the error code table.

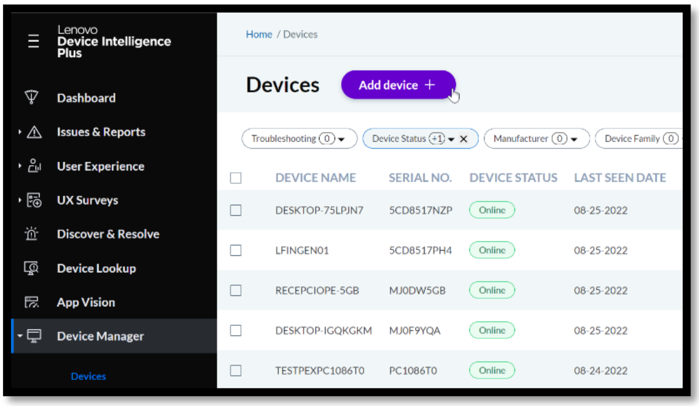


No tickets raised to Lenovo Support

This page will track manual and auto tickets generated in your fleet. Enable Auto Tickets by Creating a Service Group

2.1.7 Onboard Fleet from Devices Page (Optional)

You can also onboard the fleet of devices in your organization to LDI platform from the **Devices** page.



□	DEVICE NAME	SERIAL NO.	DEVICE STATUS	LAST SEEN DATE
□	DESKTOP-75LPJN7	5CD8517NZP	Online	08-25-2022
□	LFINGEN01	5CD8517PH4	Online	08-25-2022
□	RECEPCIOPE-5GB	MJ0DW5GB	Online	08-25-2022
□	DESKTOP-IGQKGKM	MJ0F9YQA	Online	08-25-2022
□	TESTPEXPC1086T0	PC1086T0	Online	08-24-2022

In the **Devices** page, click Add device + . The **Instructions & Agents** window appears. For more details, refer to Download Provisioning Package.

2.1.8 Proxy

UDC uses a security feature called certificate pinning. UDC does not support the scenario where a proxy service in your environment performs TLS inspection (decrypting and re-encrypting traffic using an alternate certificate). You must completely exclude the traffic for *.uds.Lenovo.com from the proxy or disable TLS inspection permanently for that endpoint. Please refer to your proxy service documentation for how to achieve this.

2.1.9 Current Support Matrix

- Leverages OS level proxy configuration
- Usage: Configure proxy information in OS using pac file or manual proxy setup

2.1.10 Limitations

Scenario	**Configure UDC to use proxy**	**For UDC to work and If TLS inspection is enabled**
Reaching to internet requires proxy	Use the OS level configuration * Pac file as well as manual proxy setup	In proxy server, whitelist *.uds.lenovo.com: 443 (include port 8883 if UDC agent older than 22.10.0.5)
Internet is reachable but proxy is also required to be setup	Use the OS level configuration * Pac file as well as manual proxy setup	Whitelist *.uds.lenovo.com at device level OR Whitelist *.uds.lenovo.com at proxy server

Note: The UDC agent installation is not supported on virtual machines, hence Type 1 hypervisors and type 2 hypervisors are not supported.

2.1.11 Troubleshooting

When you are unable to register your device in the LDI Plus tool, you can run a tool that executes some routine checks, collect logs, and other device information that can be used to analyse the problem offline. Use the LenovoDeviceIntelligence.diagcab file for troubleshooting, which you get with the Provisioning Package.

2.1.11.1. Pre-install Validation

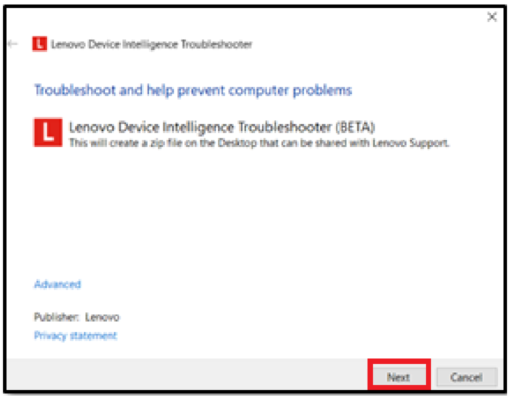
Note the following information for the API accessibility in different settings:

API Reachability	Test-NetConnection-Port 443 api.naea1.uds.lenovo.com Test-NetConnection-Port 443 api.euwe1.uds.lenovo.com

2.1.11.2. Troubleshooting Process

Follow these steps to troubleshoot:

1. Double-click the LenovoDeviceIntelligence.diagcab file. The following window appears.



Lenovo Device Intelligence Troubleshooter

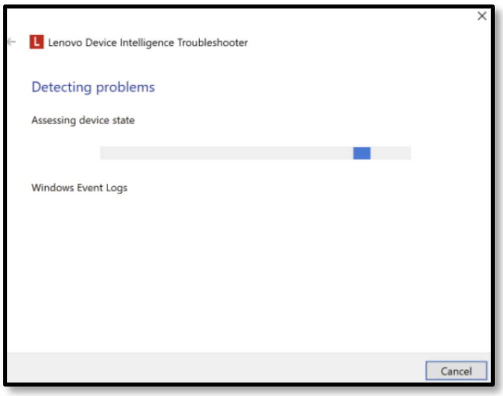
Troubleshoot and help prevent computer problems

Lenovo Device Intelligence Troubleshooter (BETA)
This will create a zip file on the Desktop that can be shared with Lenovo Support.

Advanced

Publisher: Lenovo
Privacy statement

2. Click **Next** to complete the installation.



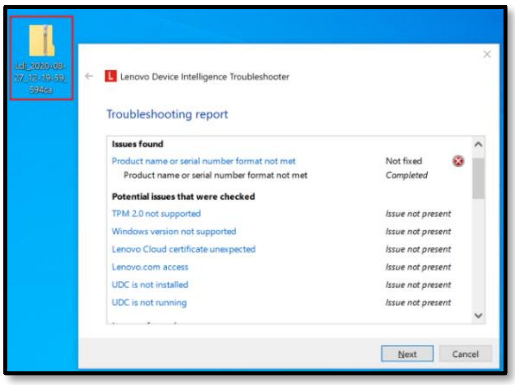
Lenovo Device Intelligence Troubleshooter

Detecting problems

Assessing device state

Windows Event Logs

4. After successful installation, the **Troubleshooting report** window appears.


ldi_2020-08-27_12-19-59_594ca
Lenovo Device Intelligence Troubleshooter
Next
Cancel

Troubleshooting report

Issues found	
Product name or serial number format not met	Not fixed
Product name or serial number format not met	*Completed*
Potential issues that were checked	
TPM 2.0 not supported	*Issue not present*
Windows version not supported	*Issue not present*
Lenovo Cloud certificate unexpected	*Issue not present*
Lenovo.com access	*Issue not present*
UDC is not installed	*Issue not present*
UDC is not running	*Issue not present*

Note: By default, the output is a zip file, and it also displays the location where the file is saved.

2.1.11.3. Level 1 Troubleshooting

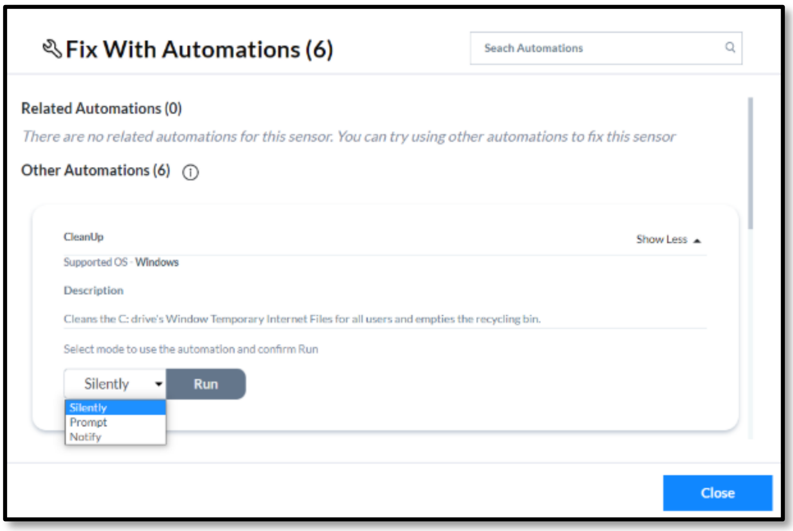
Issue Description	Troubleshooting Process
Device Status - **Pending**	After onboarding your LDI Plus device if you see the device status is **Pending**, we recommend you restart the Universal Device Client service or your LDI Plus device. To restart the UDC client, select **Services**, search for **Universal Device Client Service**, and then **Restart**. Ensure that you have an active internet connection with access to *.uds.lenovo.com ports 443 (include port 8883 if UDC agent older than 22.10.0.5) and *.lakesidesoftware.com port 443. You see the Device Status as **Pending,** if there is no license assigned to it or if the license for your device is expired, you will need to assign a license: • Click the **Unactivated** link and then click **Assign License**. or Click your profile image and select **Organization Account → Licenses → Assignments.**
Device Status - **Offline**	You see the Device Status **Offline** if the device is unable to reach the cloud for more than 5 minutes. Ensure that your LDI Plus device has an active internet connection with access to *.uds.lenovo.com port 443 (include

	port 8883 if UDC agent older than 22.10.0.5) and *.lakesidesoftware.com port 443.
If the device needs a VPN or proxy configuration	Ensure that your LDI plus device allows the following domains and ports: • *.uds.lenovo.com port 443 (include port 8883 if UDC agent older than 22.10.0.5) and *.lakesidesoftware.com port 443
Other Installation Issues	Provisioning Packs have a limited number of installations and expiration time. If you face an issue after using the same installation files for a while, select **Help & Resources à Instructions and Agents** to create a new Provisioning Pack for installations.

2.1.11.4. Device Lookup for Remediation Automation

You can use the **Fix with Automations** feature for remediation automation.

1. Log in to LDI Plus.
2. Create your automations in Configuration → Insights & Automations.
3. Select **Device Lookup → Overview** and search for a device which has an issue.
4. In the Critical Sensors section, click the Fix with Automations link.



Fix With Automations (6)

Related Automations (0)

There are no related automations for this sensor. You can try using other automations to fix this sensor

Other Automations (6)

CleanUp

Supported OS - Windows

Description

Cleans the C: drive's Window Temporary Internet Files for all users and empties the recycling bin.

Select mode to use the automation and confirm Run

Related Automations section displays the sensor-related automations whereas **Other Automations** section displays other automation besides the sensor ones.

5. Click the **Run** drop-down list.

Note: You can select one of the following modes:

Silently – You can run the automation without sending any notifications to the user's device. You see the message **Automation run successfully** in end. Select **Device Lookup → Tools → Automation History** to see the details of the execution of the remediation automation such as run from, run by, automation time, related sensors, etc.

Prompt – You send a notification to the device and the device user needs has the option to select the prompt message to start the execution of remediation automation. Select **Configuration → Insights & Automations → Automations → Automations**. In the **Prompt** text box, enter the message that you want to notify the user.

Notify - You send a notification to the device about the execution of the remediation automation. The device user has no option to cancel the notification message.

Note: This feature is available for Virtual Machines and Windows (Physical) devices only and not for macOS devices as of now.

2.1.12 Install the Agent to a Virtual Machine

1. Follow instructions in Download Provisioning Package.
2. Click **Confirm**. The **Instructions & Agents** page appears.
3. Click **Download**.
4. Copy the following files to an empty folder in the virtual device, e.g., C:\temp\LDI
   - Install-ldi.bat
   - README.txt
   - Install-ldiagent.ps1
   - Setup.exe
   - SysTrackCloudEdition.msi
   - VC_redist.x64.exe
   - VC_redist.x86.exe
5. Execute the batch file as an Administrator.
   - Open the command prompt as an administrator and execute cd C:\temp\LDItemp
   - Execute .\Install-ldi.bat

Note: Restart the device and wait for six hours for the device sync up and remain connected to network.

6. In the **Device Lookup** page, enter the virtual machine name in the **Search** text box to see the details.

2.1.13 Install the Agent to a macOS Device

Note: You can bulk deploy macOS LDI Plus devices using an endpoint manager tool.

1. Follow instructions in Download Provisioning Package.
2. Click **Confirm**. The Instructions & Agents page appears.
3. Click Download.

Note: Once downloaded, complete the following additional steps to onboard device.

4. Run Install-Ldiagent.pkg.
5. Run the below command to complete the install.

```
sudo /Library/Application\ Support/Lakeside\ Software/lsiagentctl setup
```

6. Restart the device and wait for up to a hour for the device sync up.
7. In the **Device Lookup** page, enter the macOS device name in the **Search** text box to see the details.

2.1.14 Install the LDI Agent to macOS Devices using MDM / JAMF

1. Follow instructions in Download Provisioning Package.
2. Click **Confirm**. The Instructions & Agents page appears.
3. Click Download.

Note: Once downloaded, complete the following additional steps to deploy using JAMF

4. Unzip "MacOS-install-agent" and copy the two files (Install-Agent.pkg and lsiagent.cfg) onto the desktop.
5. Create a new flat .pkg file that contains Install-Agent.pkg and lsiagent.cfg within a tmp directory. Start by creating a temp folder on your desktop:
   ```
   mkdir ~/Desktop/tmp
   ```
3. Then copy the two files(Install-Agent.pkg and lsiagent.cfg) into the new tmp folder:
   ```
   mv ~/Desktop/Install-Agent.pkg ~/Desktop/tmp
   mv ~/Desktop/lsiagent.cfg ~/Desktop/tmp
   ```
4. We will now build the package for JAMF / MDM deployment:
   ```
   pkgbuild --root ~/Desktop/tmp \
       --identifier com.example.systrack \
       --version 1.0 \
       --install-location / \
       ~/Desktop/SysTrackInstaller.pkg
   ```
5. Feel free to remove the temporary folder:
   ```
   rm -r ~/Desktop/tmp
   ```
6. Add a post-install script to the deployment package with the following commands:
   a. Run a silent install of the SysTrack Installer:
   ```
   sudo installer -pkg /tmp/Lakeside/Install-SysTrack.pkg -target /
   ```

b. Run the lsiagentctl control script
   ```
   sudo /Library/Application\ Support/Lakeside\ Software/lsiagentctl setup
   ```

2.1.15 Check LDI Agent status and restart (macOS)

The control script must be run as root or with sudo.

Check usage options:

```
sudo /Library/Application\ Support/Lakeside\ Software/lsiagentctl start
Usage: ./lsiagentctl {start|stop|restart|status}
```

Check the status of the agent:

```
root# ./lsiagentctl status
lsiagentd (pid 999) is running...
```

Restart the agent:

```
root# ./lsiagentctl restart
```

Restarting lsiagentd... done!

2.1.16 Install the LDI Agent to a Linux Device

Note: You can bulk deploy Linux LDI Plus devices using an endpoint manager tool.

1. Follow instructions in Download Provisioning Package.
2. Click **Confirm**. The Instructions & Agents page appears.
3. Click Download.

Note: Once downloaded, complete the following additional steps to onboard device.

4. Navigate to the extracted location and change the rights of *SystemsManagementAgentLinux.sh* to all read, write, and executable.

   The control script must be run as root or with sudo.

   ```
   sudo chmod ugo=wrx ./SystemsManagementAgentLinux.sh
   ```

Note: *ls -lg* will allow you to check the current rights for that file

5. Install the Agent by running the *SystemsManagementAgentLinux.sh* script with the below parameters as needed.

   The control script must be run as root or with sudo.

   ```
   sudo ./SystemsManagementAgentLinux.sh install [proxy_params]
   ```

Script Parameters	Description	Example
install	Required – Must be first parameter	N/A
--config	Optional – Default SysTrack Configuration	SysTrack Test Config
--proxyconnectionhub	Optional – The name of their ProxyConnectionHub system (if applicable)	test.lakesidesoftware.org
--autodetectproxy	Optional – Preferred proxy setting: whether or not to use autodetect	N/A
--autoconfigscript	Optional – Preferred proxy setting: the address of a .pac file from which to get proxy information	http://test.lakesidesoftware.org/test.pac
--httpproxy	Optional – Preferred proxy setting: the address for the preferred HTTP proxy	127.0.0.1:80
--httpsproxy	Optional – Preferred proxy setting: the address for the preferred HTTPS proxy	127.0.0.1:443
--ftpproxy	Optional – Preferred proxy setting: the address for the preferred FTP proxy	127.0.0.1:21
--socketproxy	Optional – Preferred proxy setting: the address for the preferred Socket proxy	127.0.0.1:443

6. Restart the device and wait for up to a hour for the device sync up.
7. In the **Device Lookup** page, enter the Linux device name in the **Search** text box to see the details.

2.1.17 Uninstall LDI Agent (Windows)

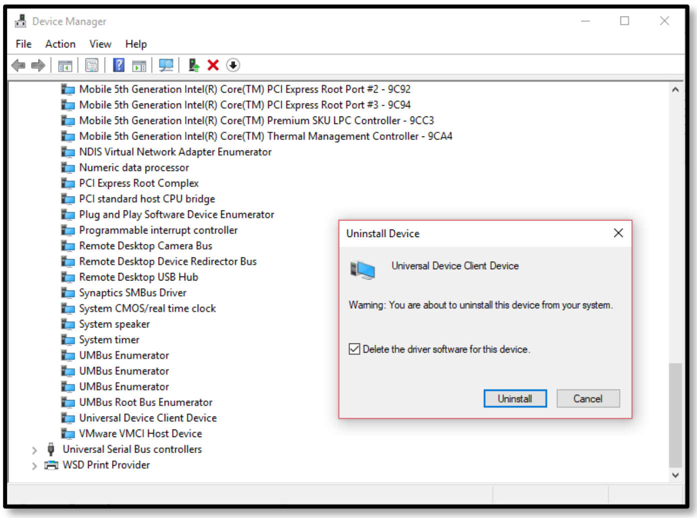
Note: We recommend you use the Device Manager option to uninstall Universal Device Client (UDC) that ensures removal of UDC from both Windows and Driver Store.

1. In the device, open the **Device Manager** page.
2. Select **System devices** and right-click **Universal Device Client Device**.
3. Select **Uninstall.**

   Note:

   - Select the **Delete the driver software for this device** check box.
   - Continue to remove SysTrack as described below if the device is an LDI Plus.
4. Open Settings or Control Panel in your system to uninstall Systems Management Agent.

- **Settings → Add or Remove Programs → Systems Management Agent → Uninstall**
- **Control Panel → Programs and Features → Systems Management Agent → Uninstall**


Device Manager
File
Action
View
Help
Mobile 5th Generation Intel(R) Core(TM) PCI Express Root Port #2 - 9C92
Mobile 5th Generation Intel(R) Core(TM) PCI Express Root Port #3 - 9C94
Mobile 5th Generation Intel(R) Core(TM) Premium SKU LPC Controller - 9CC3
Mobile 5th Generation Intel(R) Core(TM) Thermal Management Controller - 9CA4
NDIS Virtual Network Adapter Enumerator
Numeric data processor
PCI Express Root Complex
PCI standard host CPU bridge
Plug and Play Software Device Enumerator
Programmable interrupt controller
Remote Desktop Camera Bus
Remote Desktop Device Redirector Bus
Remote Desktop USB Hub
Synaptics SMBus Driver
System CMOS/real time clock
System speaker
System timer
UMBus Enumerator
UMBus Enumerator
UMBus Enumerator
UMBus Root Bus Enumerator
Universal Device Client Device
VMware VMCI Host Device
Universal Serial Bus controllers
WSD Print Provider
Uninstall Device
Uninstall
Cancel

Universal Device Client Device

Warning: You are about to uninstall this device from your system.

☑ Delete the driver software for this device.

5. Verify that there is no Universal Device Client Service in Device Manager or running service.
6. Restart the device.
7. In the LDI Plus portal, select **Device Manager → Devices**, search for that device and click **Delete**.

2.1.18 Uninstall LDI Agent with scripts (Windows)

Automated uninstall using Powershell

```
# This will uninstall UDC device, service, driver, & data
# Ensure running with elevated privileges
$udcInstall = Get-Item (Join-Path ([System.Environment]::SystemDirectory)
"drivers\Lenovo\udc\Data\InfBackup\UDCInfInstaller.exe")
if($null -eq $udcInstall) { throw "Unable to locate UDC install files" }
Push-Location $udcInstall.Directory.FullName
& $udcInstall.Fullname -uninstall
Pop-Location
```

Automated uninstall using Cmd

```
:: This will uninstall UDC device, service, driver, & data
:: Ensure running with elevated privileges
PUSHD %windir%\System32\drivers\Lenovo\udc\Data\InfBackup\
.\UDCInfInstaller.exe -uninstall
POPD
```

2.1.19 Uninstall LDI Agent (macOS)

To uninstall the LDI agent from a macOS device, run the below script in the macOS terminal

The control script must be run as root or with sudo.

```
sudo /Library/Application\ Support/Lakeside\ Software/uninstall_systrack.sh
```

2.1.20 Uninstall LDI Agent (Linux)

To uninstall the LDI agent from a Linux device, run the below script in the Linux terminal

The control script must be run as root or with sudo.

```
sudo ./SystemsManagementAgentLinux.sh remove
```

2.1.21 Additional Information

Following are some of the issues and their resolutions regarding virtual machine and macOS device installation:

Issue 1: Virtual machine/macOS is not onboarded to LDI Plus device.

Resolution: Verify that the correct version of installer is downloaded from the LDI Plus portal.

Issue 2: Virtual Machine/macOS is not found in the Device Lookup page.

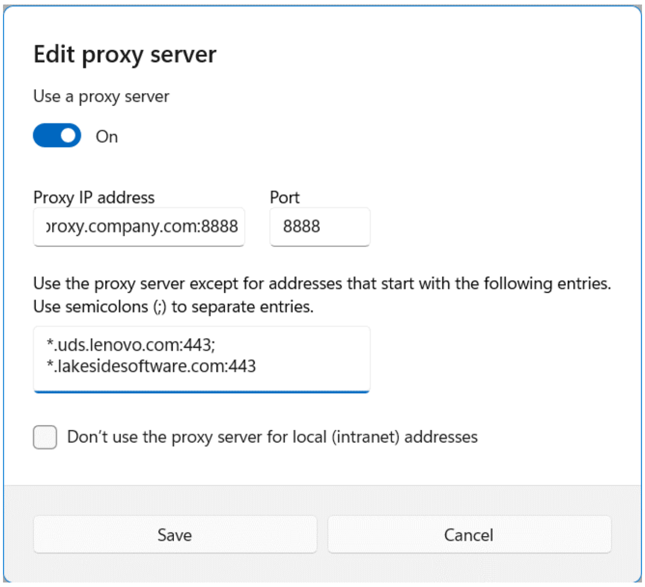
Resolution: Wait for six hours after restarting your machine.

2.1.22 Onboard Your Fleet in a Proxy Environment

You can onboard your device using proxy setups.

Manual Proxy Setup section:

1. In the **Address** field, enter https=exampleproxy.company.com:8888
2. In the **Port** field, enter **8888**.



Edit proxy server

Use a proxy server

On

Proxy IP address: ›roxy.company.com:8888

Port: 8888

Use the proxy server except for addresses that start with the following entries. Use semicolons (;) to separate entries.

*.uds.lenovo.com:443;
*.lakesidesoftware.com:443

□ Don't use the proxy server for local (intranet) addresses

UDC and LDI Plus support the following proxy configurations:

- You must configure proxy through WinINet (vs WinHTTP or a 3rd party application / browser extension)
- Proxy server can reach *.uds.lenovo.com:443 (include port 8883 if UDC agent older than 22.10.0.5) and *.lakesidesoftware.com:443
- Proxy server does DNS resolving for client
- Proxy server does NOT support authentication.

Note: UDC can register and sync telemetry on proxy environment by auto-detect the browser proxy settings (except if a user/password is required for such proxy access, which it is not supported).

UDC always imports whatever is configured in the browser settings (WinINet) automatically, though manual setting is done for WinHTTP.

2.2 LDI Plus SCCM Quick Start Guide

2.2.1 Overview

The LDI Plus SCCM QSG chapter explains how to use System Center Configuration Manager (SCCM) to deploy the LDI Provisioning Package on the fleet of devices in your organization.

You can use following methods to deploy the package:

- Configure SCCM to deploy LDI Windows (Physical) Package on the Devices in the **Application Mode**
- Configure SCCM to deploy LDI Windows (Physical) Package on the Devices in the **Package Mode**

2.2.2 Purpose

You can configure SCCM to install the LDI Provisioning Package on all the devices in your organization and register them as per the Service License Agreement between your organization and LDI Solutions. Instead of installing the provisioning package on each device, you can use SSCM to run it on the entire fleet of device.

2.2.3 Prerequisite

Download the LDI Provisioning Package on the device on which you want to configure SCCM and deploy the package on the entire fleet of devices in your organization. To know how to download and install the package, refer to Onboard Your Fleet.

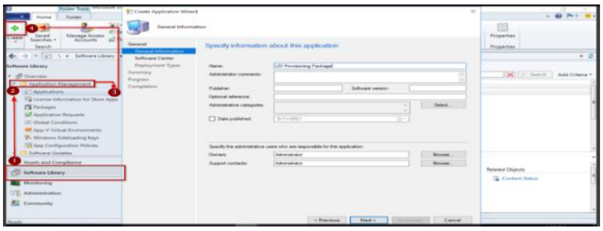
2.2.4 Configure SCCM to Deploy LDI Windows (Physical) Package on the Devices in the Application Mode

2.2.4.1. Create an Application

Copy the following files downloaded from the LDI Windows (Physical) package to a folder in the computer with an account of the site server that has READ permission.

- Udc_setup.exe
- LenovoDeviceIntelligence-0.0.75.0.diagcab
- README.txt

- install-ldi.bat



Specify information about this application

Name: LDI Provisioning Package

Owners: Administrator

Support contacts: Administrator

In the SCCM account:

1. Click the **Software Library** tab. The Software Library window appears.
2. Click the **Applications Management** folder. The Application window appears.
3. Click **Applications**.

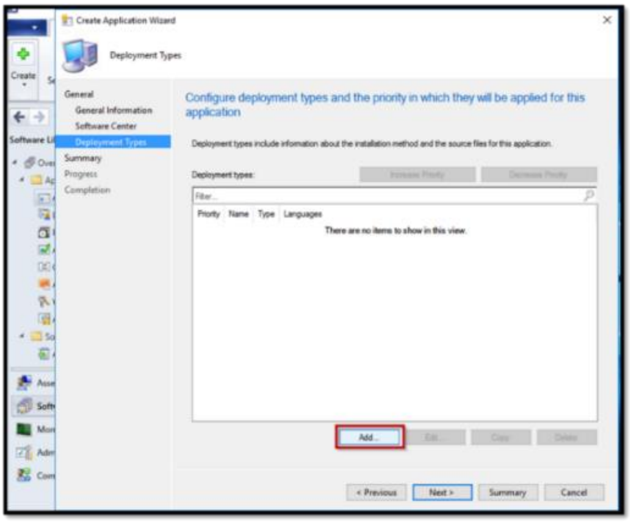
Create Application Wizard

Enter information about a new application in the SCCM. Fill-in the name, version, and publisher of the application. You can also select the administrative owners (users) and category of the application.

4. Click **Create**. The **Create Application** window appears.
5. Click **Next**. The **Deployment Types** page appears.

The new application is registered in SCCM. The next section **Deploy the Application** describes the steps to deploy the new application.

2.2.4.2. Add Deployment Type to the Application



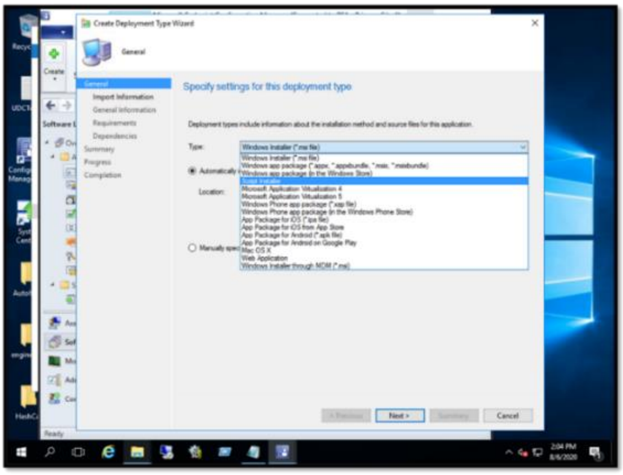
Configure deployment types and the priority in which they will be applied for this application

Deployment types include infomation about the installation method and the source files for this application.

There are no items to show in this view.

In the **Deployment Types** page, click **Add** and then click **Next.** A window appears that shows a list of options.

2.2.4.3. Select Deployment Setting



Create Deployment Type Wizard

General

Specify settings for this deployment type

Deployment types include information about the installation method and source files for this application.

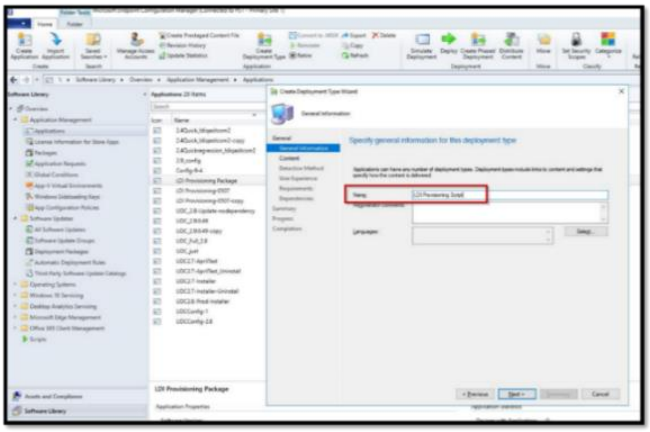
Type: Windows Installer (*.msi file)

Windows Installer (*.msi file)
Windows app package (*.appx, *.appxbundle, *.msix, *.msixbundle)
Windows app package (in the Windows Store)
Script Installer
Microsoft Application Virtualization 4
Microsoft Application Virtualization 5
Windows Phone app package (*.xap file)
Windows Phone app package (in the Windows Phone Store)
App Package for iOS (*.ipa file)
App Package for iOS from App Store
App Package for Android (*.apk file)
App Package for Android on Google Play
Mac OS X
Web Application
Windows Installer through MDM (*.msi)

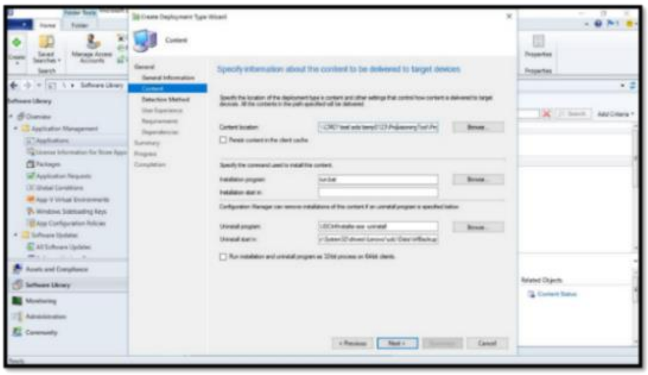
1. Select **Script Installer**.
2. Click **Next**.

2.2.4.4. Specify Content Settings for Delivery to Devices

3. Enter **Name** of the application. For example, LDI Provisioning Script.
4. Click **Next**. The Content - the Create Deployment Type window appears.

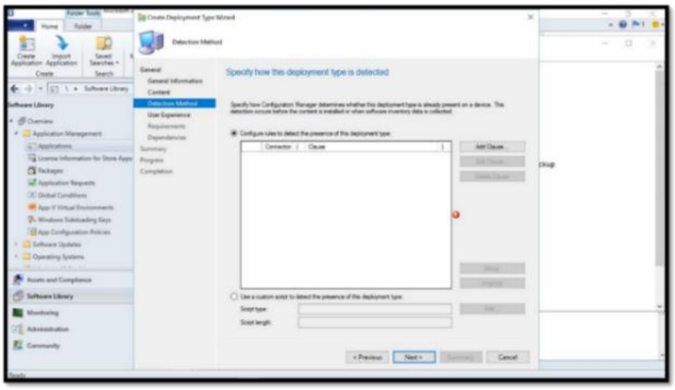


5. In the **Content** page, specify the path of the folder that has all files.



6. In the **installation program** field, enter the command - **install-ldi.bat**. If the target device is a virtual machine, then enter the command **Setup.exe /VERYSILENT**.
7. In the Uninstall program field, enter the command - UDCInfInstaller.exe -uninstall.

8. In the Uninstall start field, enter the command
   - **C:\Windows\System32\drivers\Lenovo\udc\Data\InfBackup**
9. Click **Next**. A window appears.
10. In the window, specify how the deployment type is detected.
11. Click **Add Clause.**



Create Deployment Type Wizard

Detection Method

Specify how this deployment type is detected

Specify how Configuration Manager determines whether this deployment type is already present on a device. The detection occurs before the content is installed or when software inventory data is collected.

● Configure rules to detect the presence of this deployment type

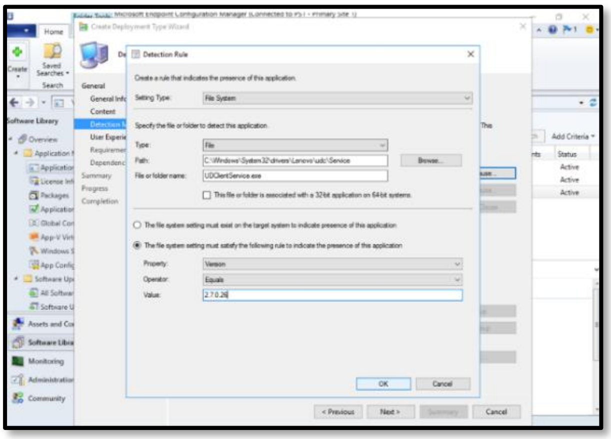
○ Use a custom script to detect the presence of this deployment type

Script type:

Script length:

12. Click **Next**. The **Detection Rule** window appears.

2.2.4.5. Specify Detection Rule



Detection Rule

Create a rule that indicates the presence of this application.

Setting Type: File System

Specify the file or folder to detect this application.

Type: File

Path: C:\Windows\System32\drivers\Lenovo\udc\Service

File or folder name: UDClientService.exe

□ This file or folder is associated with a 32-bit application on 64-bit systems.

○ The file system setting must exist on the target system to indicate presence of this application

● The file system setting must satisfy the following rule to indicate the presence of this application

Property: Version

Operator: Equals

Value: 2.7.0.26

In the **Detection Rule** window, configure the detection rules as follows:

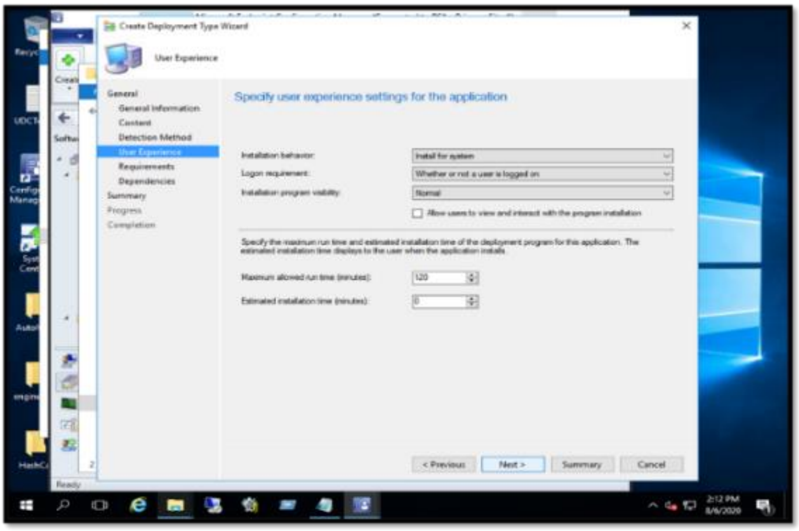
1. In the **Setting Type** field, select **File System**.
2. In the **Path** field, enter C:\Windows\System32\drivers\Lenovo\udc\Service**.**
3. In the **File or folder name** field, enter UDClientService.exe
4. Note: De-select the This file or folder is associated with a 32-bit application on 64-bit system checkbox.
5. Select The file system setting must satisfy the following rule to indicate the presence of this application radio button.
6. In the **Property** drop-down list, select **Version**.

7. In the **Operator** drop-down list, select **Equals**.
8. In the **Value** field, enter the current UDC version.
9. Click **OK**.
10. Click **Next**.

2.2.4.6. Configure User Experience Settings

In the **User Experience** page, follow these steps:

1. In the Installation behavior field, select **Install for a system**.
2. In the Logon requirement field, select **Whether or not a user is logged on**.
3. In the Installation program visibility field, select **Normal**.
4. Click **Next.**



Create Deployment Type Wizard

User Experience

Specify user experience settings for the application

Installation behavior: Install for system

Logon requirement: Whether or not a user is logged on

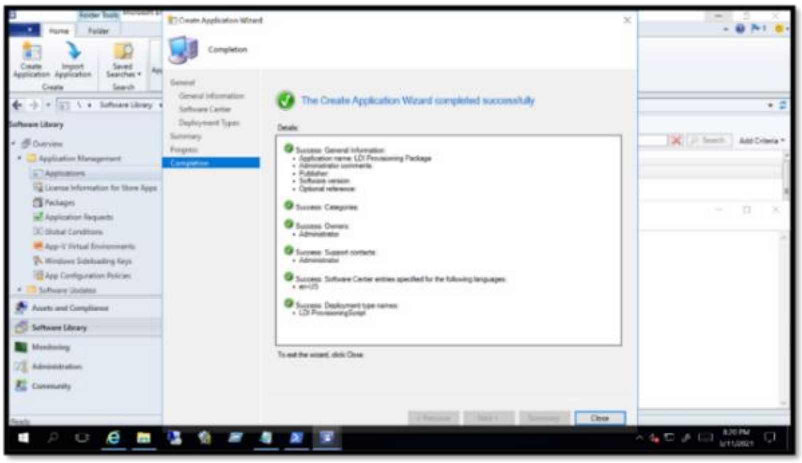
Installation program visibility: Normal

□ Allow users to view and interact with the program installation

Specify the maximum run time and estimated installation time of the deployment program for this application. The estimated installation time displays to the user when the application installs.

Maximum allowed run time (minutes): 120

Estimated installation time (minutes): 0



Create Application Wizard

Completion

The Create Application Wizard completed successfully

Details:

Success: General Information
- Application name: LDI Provisioning Package
- Administrator comments:
- Publisher:
- Software version:
- Optional reference:

Success: Categories

Success: Owners:
- Administrator

Success: Support contacts:
- Administrator

Success: Software Center entries specified for the following languages:
- en-US

Success: Deployment type names:
- LDI ProvisioningScript

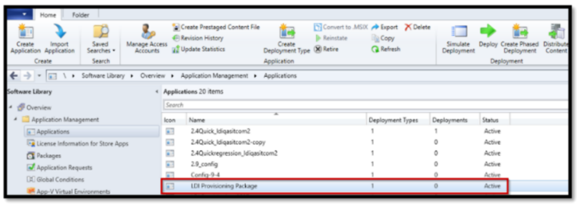
To exit the wizard, click Close.

Complete the rest of the wizard to create the deployment type for the application.

2.2.4.7. Deploy the LDI Provisioning Package in SCCM to the Fleet of Devices

After you register the LDI provisioning pack and configure the deployment settings in the SCCM account, you must deploy or assign the application to a group or fleet of devices in the organization.

2.2.4.8. Select Application for Deployment to the Device Group

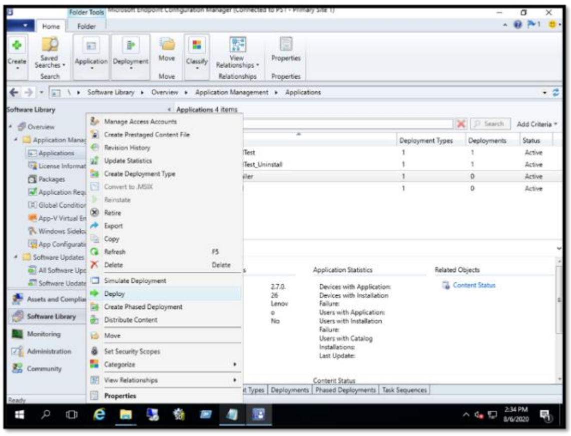


\ ▸ Software Library ▸ Overview ▸ Application Management ▸ Applications

Applications 20 items

Icon	Name	Deployment Types	Deployments	Status
	2.4Quick_ldiqasitcom2	1	1	Active
	2.4Quick_ldiqasitcom2-copy	1	0	Active
	2.4Quickregression_ldiqasitcom2	1	0	Active
	2.9_config	1	0	Active
	Config-9-4	1	0	Active
	LDI Provisioning Package	1	0	Active

5. Select the application. For example, LDI Provisioning Package.
6. Right-click the selected application**.** A pop-up window appears.



\ ▸ Software Library ▸ Overview ▸ Application Management ▸ Applications

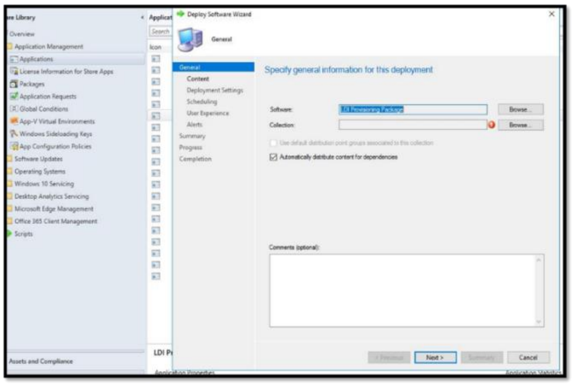
Applications 4 items

	Deployment Types	Deployments	Status
Test	1	1	Active
Test_Uninstall	1	1	Active
ller	1	0	Active
	1	0	Active

2.7.0.
26
Lenov
0
No

Devices with Application:
Devices with Installation Failure:
Users with Application:
Users with Installation Failure:
Users with Catalog Installations:
Last Update:

7. Click **Deploy.**



Specify general information for this deployment

Software: LDI Provisioning Package

Collection:

□ Use default distribution point groups associated to this collection

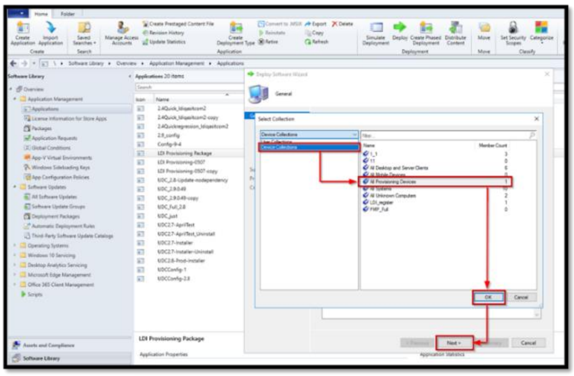
☑ Automatically distribute content for dependencies

Comments (optional):

In the **General** page in the **Deploy Software Wizard**:

8. Click **browse** to select the software package. For example, LDI Provisioning Package.

9. In the **Collection** field, click **browse**. The **Select Collection** window appears.

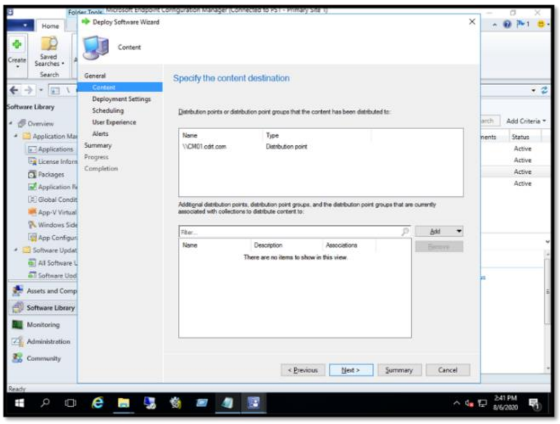


10. In the **Select Collection** window, **click Device Collections.** A list of device collections appears.

> Device Collection
>
> The fleet or group of devices. For example, the fleet of devices in your organization that is to be onboarded to the LDI platform.

2.2.4.9. Specify Content Destination

1. Specify the distribution point where the collection of devices is to be deployed.
2. Click **Next.**



Specify the content destination

Distribution points or distribution point groups that the content has been distributed to:

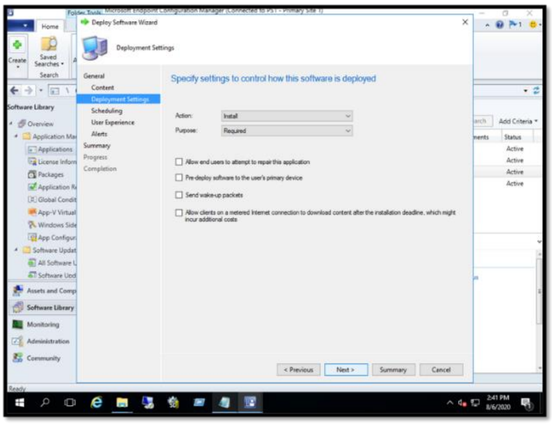
Name	Type
\\CM01.cdt.com	Distribution point

Additional distribution points, distribution point groups, and the distribution point groups that are currently associated with collections to distribute content to:

Name	Description	Associations

There are no items to show in this view.

3. Select the deployment settings for the software. For example, LDI Provisioning Package.



Specify settings to control how this software is deployed

Action: Install

Purpose: Required

□ Allow end users to attempt to repair this application

□ Pre-deploy software to the user's primary device

□ Send wake-up packets

□ Allow clients on a metered Internet connection to download content after the installation deadline, which might incur additional costs

4. In the **Action** field, select **Install.**
5. in the **Purpose** field, select **Required.**

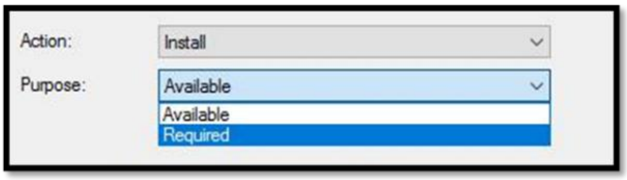
> **Mandatory**
>
> Select the **Required** option to install UDC Installer software.

2.2.4.10. Known Issues

Error Code	Error Description	Root Cause	Workaround
0x87D00324	When you test the SCCM deployment, a notification **Installation Failed** appears on end user's desktop, however the package is installed successfully.	The software detection rule was not found.	In the **Deploy Software Wizard** page, select **User Experience**. Then, in the **User notifications** drop-down list, select **Hide in Software Center and all notifications.**

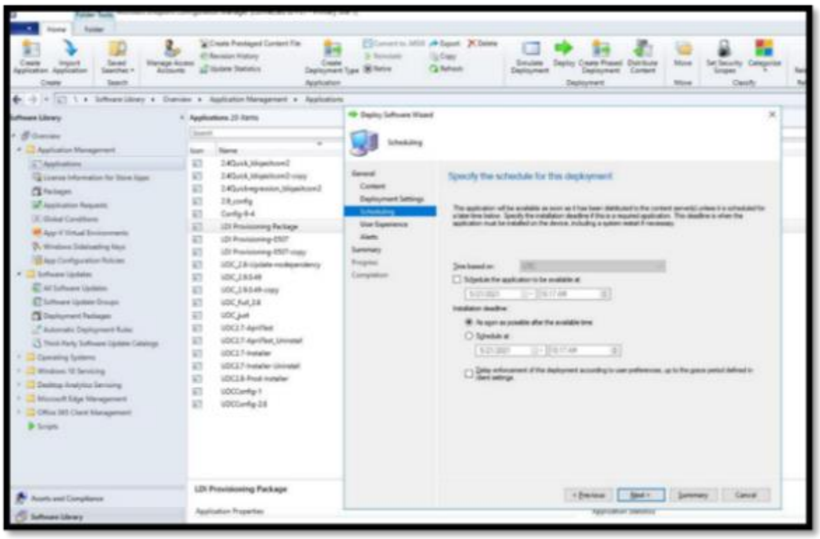
2.2.5 Scheduling

Leave the Scheduling settings as default.



Action: Install

Purpose: Available



Deploy Software Wizard

Scheduling

Specify the schedule for this deployment

The application will be available as soon as it has been distributed to the content server(s) unless it is scheduled for a later time below. Specify the installation deadline if this is a required application. This deadline is when the application must be installed on the device, including a system restart if necessary.

Time based on: UTC

☐ Schedule the application to be available at: 5/21/2021 10:17 AM

Installation deadline:

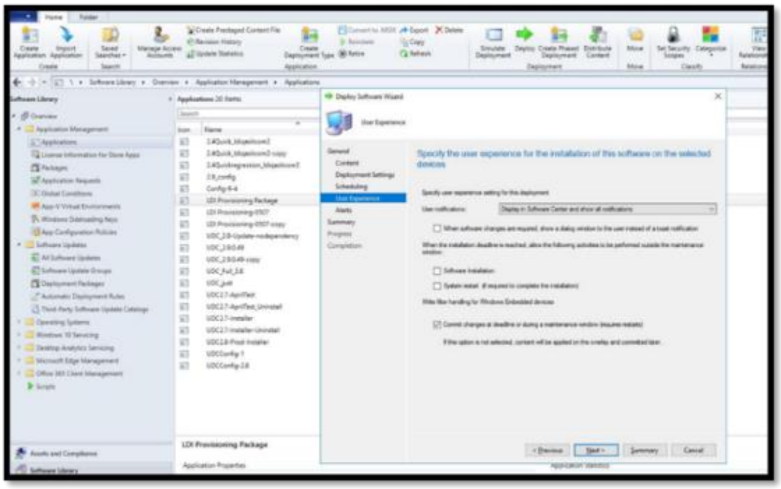
● As soon as possible after the available time

○ Schedule at: 5/21/2021 10:17 AM

☐ Delay enforcement of this deployment according to user preferences, up to the grace period defined in client settings.

2.2.6 User Experience

You are advised to leave the User Experience settings as default.



Deploy Software Wizard

User Experience

Specify the user experience for the installation of this software on the selected devices

Specify user experience setting for this deployment

User notifications: Display in Software Center and show all notifications

☐ When software changes are required, show a dialog window to the user instead of a toast notification

When the installation deadline is reached, allow the following activities to be performed outside the maintenance window:

☐ Software Installation

☐ System restart (if required to complete the installation)

Write filter handling for Windows Embedded devices

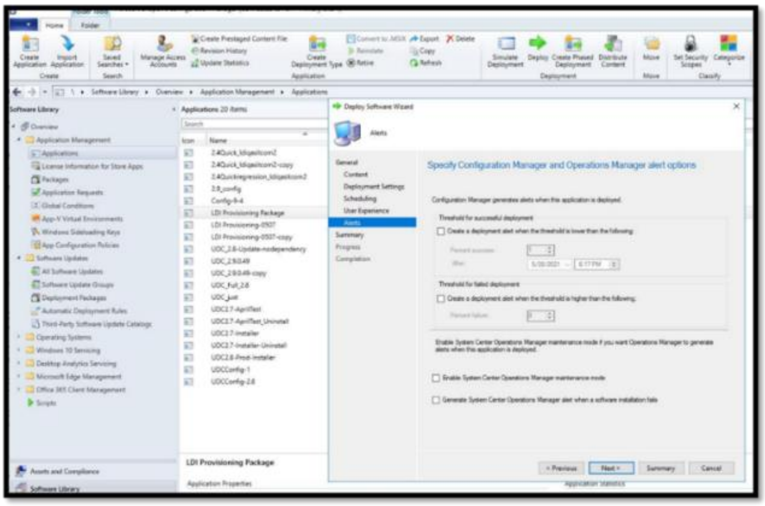
☑ Commit changes at deadline or during a maintenance window (requires restarts)

If this option is not selected, content will be applied on the overlay and committed later.

2.2.7 Alerts

You are advised to leave the Alerts settings as default. If you want to use the Alerts feature, then refer to the SCCM official user guide.

Complete the rest of the wizard to complete the deployment.



Deploy Software Wizard

Alerts

Specify Configuration Manager and Operations Manager alert options

Configuration Manager generates alerts when this application is deployed.

Threshold for successful deployment

☐ Create a deployment alert when the threshold is lower than the following:

Threshold for failed deployment

☐ Create a deployment alert when the threshold is higher than the following:

Enable System Center Operations Manager maintenance mode if you want Operations Manager to generate alerts when this application is deployed.

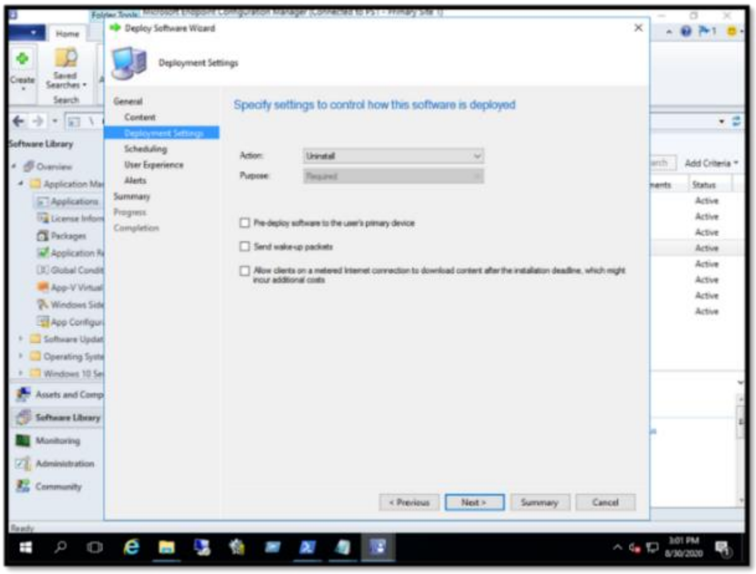
☐ Enable System Center Operations Manager maintenance mode

☐ Generate System Center Operations Manager alert when a software installation fails

Verify if the devices in the Device Collection that are deployed with this application can successfully finish the installation.

Verify in the LDI portal if the devices are successfully activated.

2.2.8 SCCM Uninstall UDC Client



Deploy Software Wizard

Deployment Settings

Specify settings to control how this software is deployed

Action: Uninstall

Purpose: Required

☐ Pre-deploy software to the user's primary device

☐ Send wake-up packets

☐ Allow clients on a metered Internet connection to download content after the installation deadline, which might incur additional costs

To uninstall the LDI Agent, for example, UDC service, follow these steps:

2.2.8.1. Select the Application to Uninstall

1. In the **Applications** tab, select the application.
2. Right-click the application.
3. Click **Deploy**.
4. Select the Group of Device.
5. Click Device Collection.
6. Select the Automatically distribute content for dependencies checkbox.

2.2.8.2. Specify Content Destination

Specify Settings to Control Software Deployment

Action: **Uninstall**

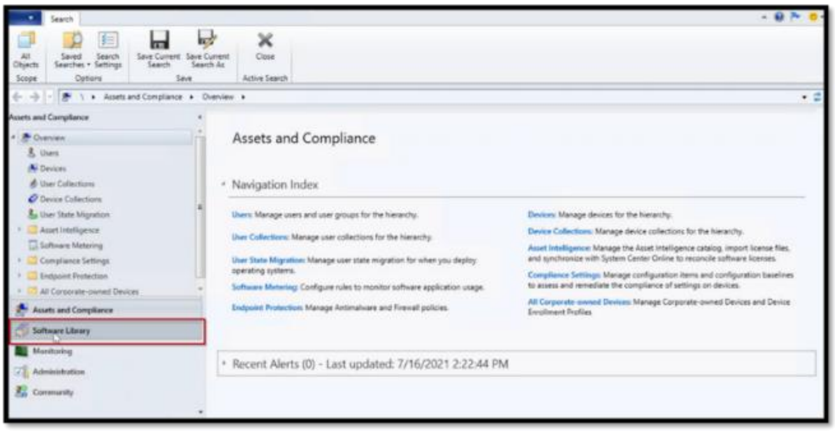
Purpose: **Required**

1. Complete the Uninstall Process.
2. Verify if the devices in the Device Collection that are deployed with this uninstall deployment, have UDC software uninstalled from them.
3. In the LDI portal, delete the devices before running the provisioning tool again.

2.2.9 Configure SCCM to Deploy LDI Windows (Physical) Package on the Devices in the Package Mode

2.2.9.1. Create a Package

1. Log in to the SCCM Account.
2. In the navigation menu, click **Software Library**. The **Software Library** window appears.



Assets and Compliance

Navigation Index

Users: Manage users and user groups for the hierarchy.

User Collections: Manage user collections for the hierarchy.

User State Migration: Manage user state migration for when you deploy operating systems.

Software Metering: Configure rules to monitor software application usage.

Endpoint Protection: Manage Antimalware and Firewall policies.

Devices: Manage devices for the hierarchy.

Device Collections: Manage device collections for the hierarchy.

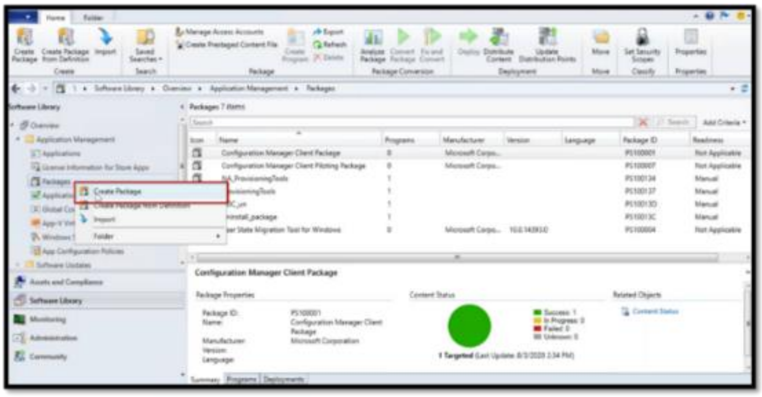
Asset Intelligence: Manage the Asset Intelligence catalog, import license files, and synchronize with System Center Online to reconcile software licenses.

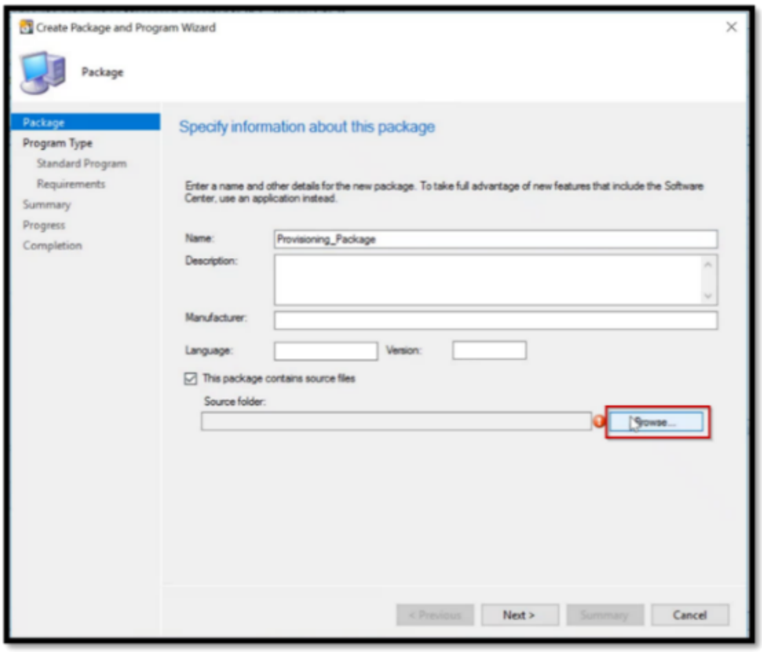
Compliance Settings: Manage configuration items and configuration baselines to assess and remediate the compliance of settings on devices.

All Corporate-owned Devices: Manage Corporate-owned Devices and Device Enrollment Profiles

Recent Alerts (0) - Last updated: 7/16/2021 2:22:44 PM

3. Click **Application Manager** folder to view the sub menu.
4. Right-click **Packages**.
5. Right-click **Create Package**. The form field appears where you can enter details about the package.





Specify information about this package

Enter a name and other details for the new package. To take full advantage of new features that include the Software Center, use an application instead.

Name: Provisioning_Package

Description:

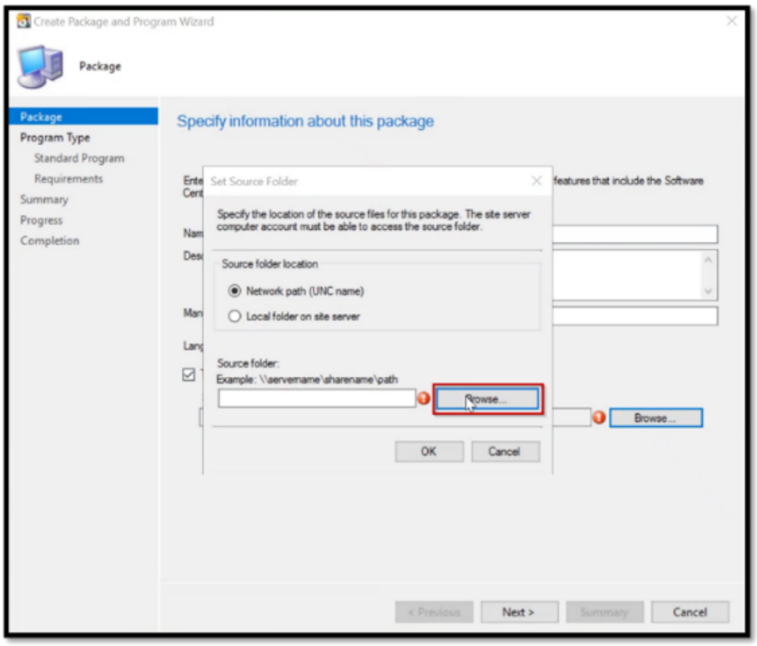
Manufacturer:

Language: Version:

☑ This package contains source files

Source folder:

6. Enter the **name** of the package. For example, Provisioning Package.
7. Select the **checkbox**. This package contains the source file.
8. Click **Browse**.



Specify information about this package

Specify the location of the source files for this package. The site server computer account must be able to access the source folder.

Source folder location

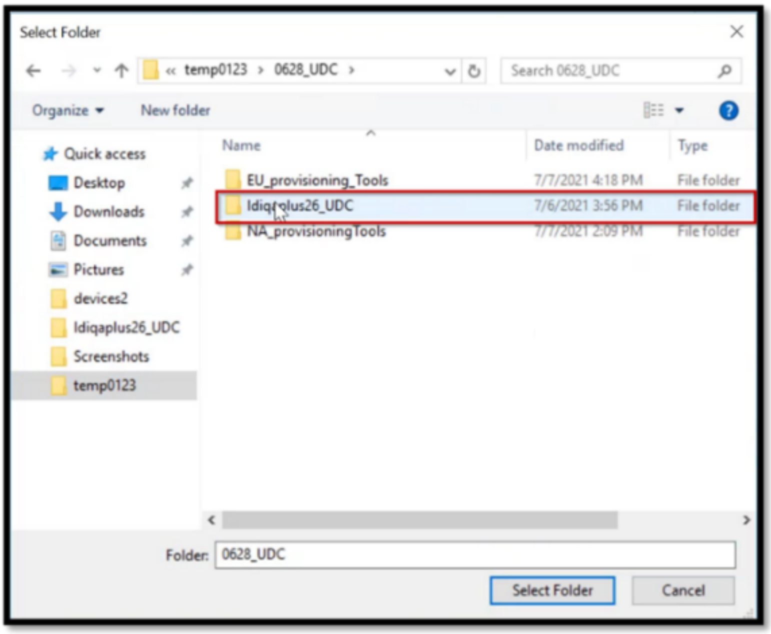
● Network path (UNC name)

○ Local folder on site server

Source folder:

Example: \\servername\sharename\path

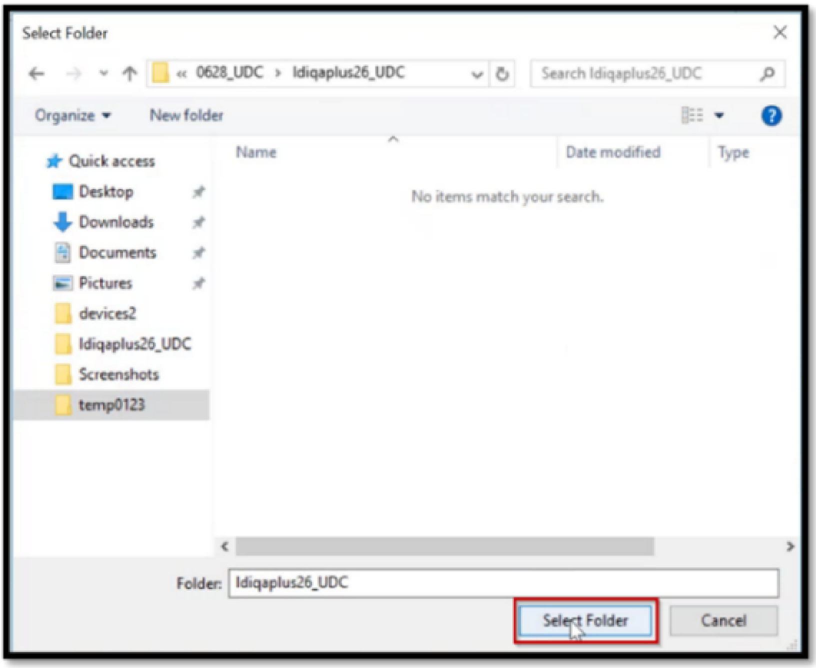
9. In the Create Package and Program Wizard window, click Browse.



Name	Date modified	Type
EU_provisioning_Tools	7/7/2021 4:18 PM	File folder
Idiqaplus26_UDC	7/6/2021 3:56 PM	File folder
NA_provisioningTools	7/7/2021 2:09 PM	File folder

Folder: 0628_UDC

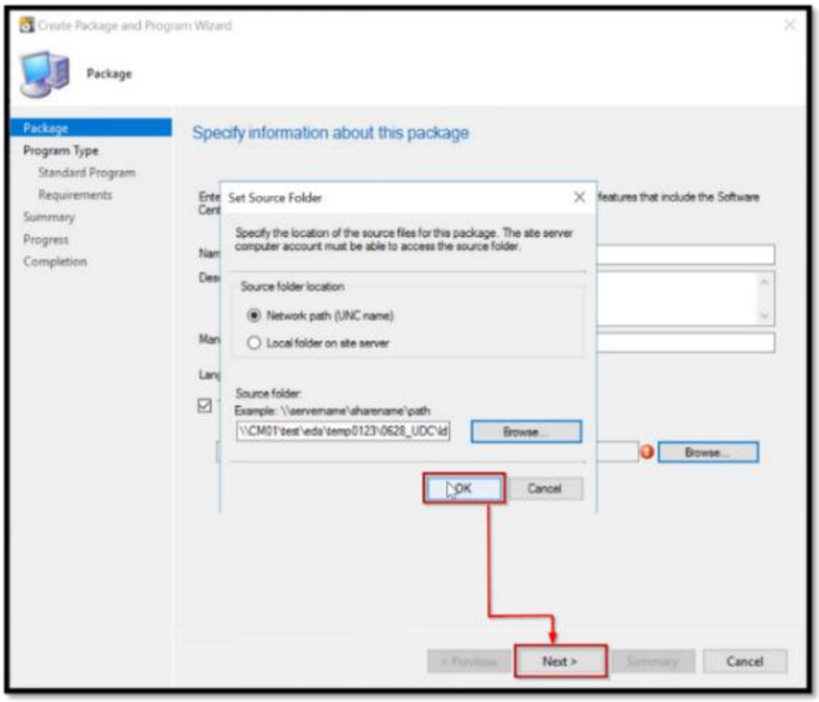
10. Select the **folder**. For example, ldiplus26_UDC.



No items match your search.

Folder: Idiqaplus26_UDC

11. Click **Select Folder**. A pop-up window appears.



Specify information about this package

Set Source Folder

Specify the location of the source files for this package. The site server computer account must be able to access the source folder.

Source folder location

● Network path (UNC name)

○ Local folder on site server

Source folder:
Example: \\servername\sharename\path

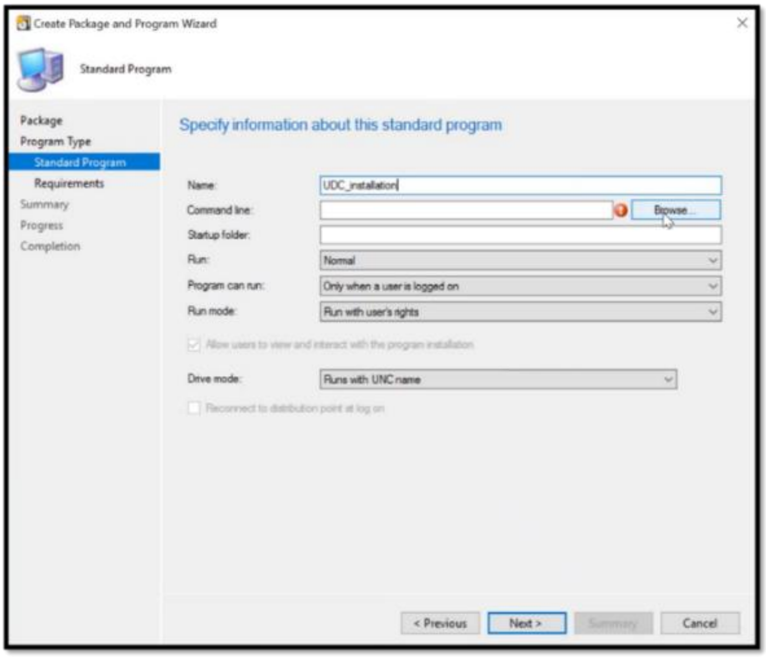
\\CM01\test\eda\temp0123\0628_UDC\ld

The window shows the path of the selected folder.

12. Click **OK**.
13. Click **Next**. In the **Program Type** section, select the type of program you want to create.

2.2.9.2. Create a Program

1. Select Standard program.
2. Select **Next**. You see form field for the creating the program.

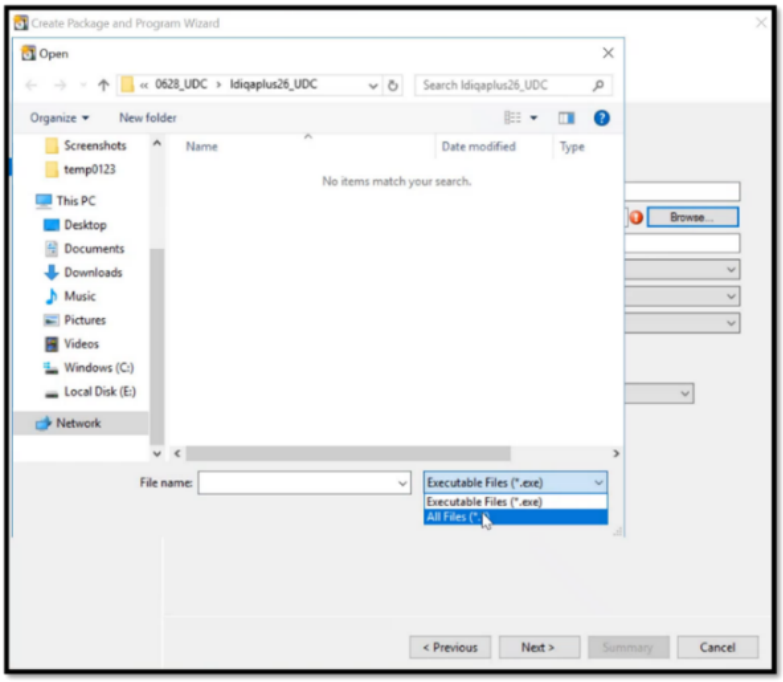


Specify information about this standard program

Name: UDC_installation
Command line:
Startup folder:
Run: Normal
Program can run: Only when a user is logged on
Run mode: Run with user's rights
☑ Allow users to view and interact with the program installation
Drive mode: Runs with UNC name
□ Reconnect to distribution point at log on

3. Enter the name of the program. For example, UDC_Installation.

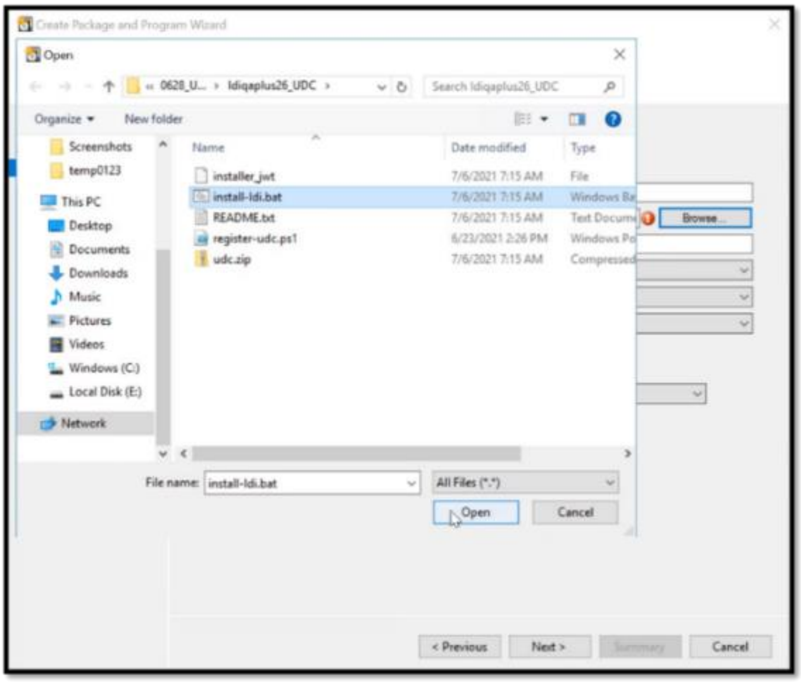
4. In the **Command line** field, click **Browse**. You see the following pop-up window.



No items match your search.

File type: Executable Files (*.exe)

5. Select **All Files**. You see all the files.



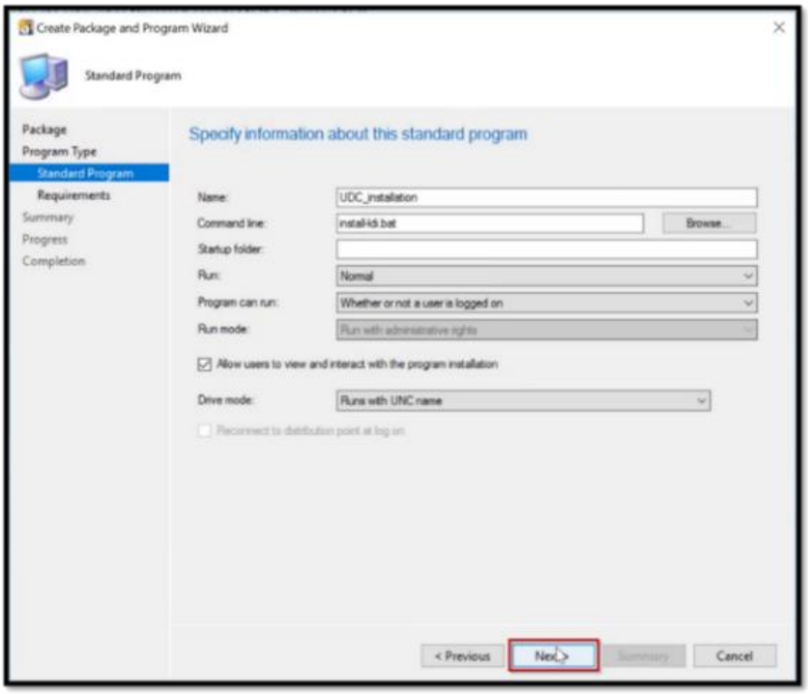
Name	Date modified	Type
installer_jwt	7/6/2021 7:15 AM	File
install-ldi.bat	7/6/2021 7:15 AM	Windows Ba
README.txt	7/6/2021 7:15 AM	Text Docum
register-udc.ps1	6/23/2021 2:26 PM	Windows Po
udc.zip	7/6/2021 7:15 AM	Compressed

File name: install-ldi.bat

All Files (*.*)

6. Select install-ldi.bat.

7. Select **Open**.



Specify information about this standard program

Name: UDC_installation

Command line: install-idi.bat

Startup folder:

Run: Normal

Program can run: Whether or not a user is logged on

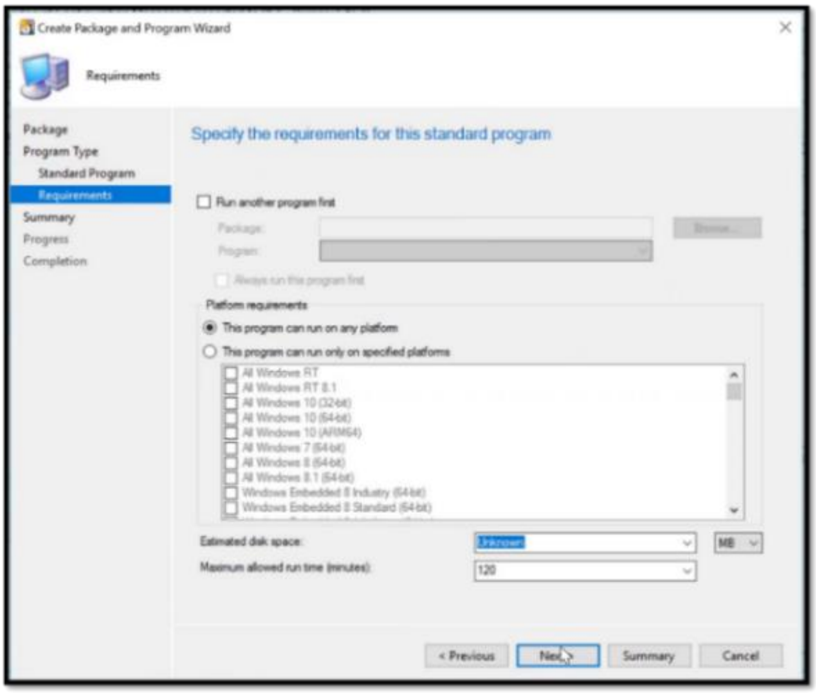
Run mode: Run with administrative rights

☑ Allow users to view and interact with the program installation

Drive mode: Runs with UNC name

□ Reconnect to distribution point at log on

8. In the Program can run field, select Whether or not a user is logged on.
9. Select the checkbox - Allow users to view and interact with the program installation.
10. Click **Next**.



Specify the requirements for this standard program

□ Run another program first

Package:

Program:

□ Always run this program first

Platform requirements

● This program can run on any platform

○ This program can run only on specified platforms

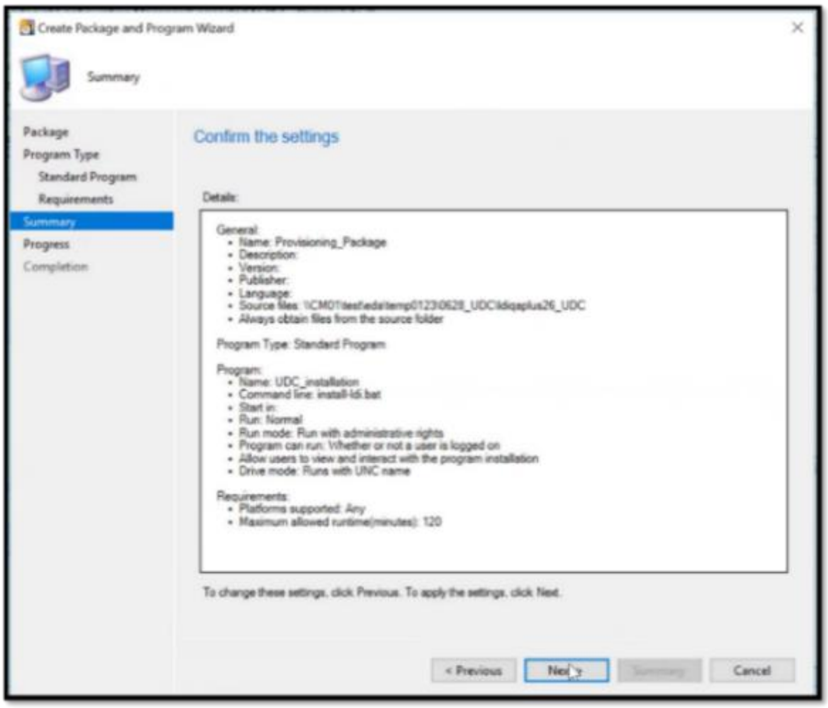
□ All Windows RT
□ All Windows RT 8.1
□ All Windows 10 (32-bit)
□ All Windows 10 (64-bit)
□ All Windows 10 (ARM64)
□ All Windows 7 (64-bit)
□ All Windows 8 (64-bit)
□ All Windows 8.1 (64-bit)
□ Windows Embedded 8 Industry (64-bit)
□ Windows Embedded 8 Standard (64-bit)

Estimated disk space: Unknown MB

Maximum allowed run time (minutes): 120

Note: In the **Requirements** section, keep the default settings, as shown in the screenshot.

11. Click **Next**.



Confirm the settings

Details:

General:
- Name: Provisioning_Package
- Description:
- Version:
- Publisher:
- Language:
- Source files: \\CM01\test\eda\temp01230628_UDC\ldiqaplus26_UDC
- Always obtain files from the source folder

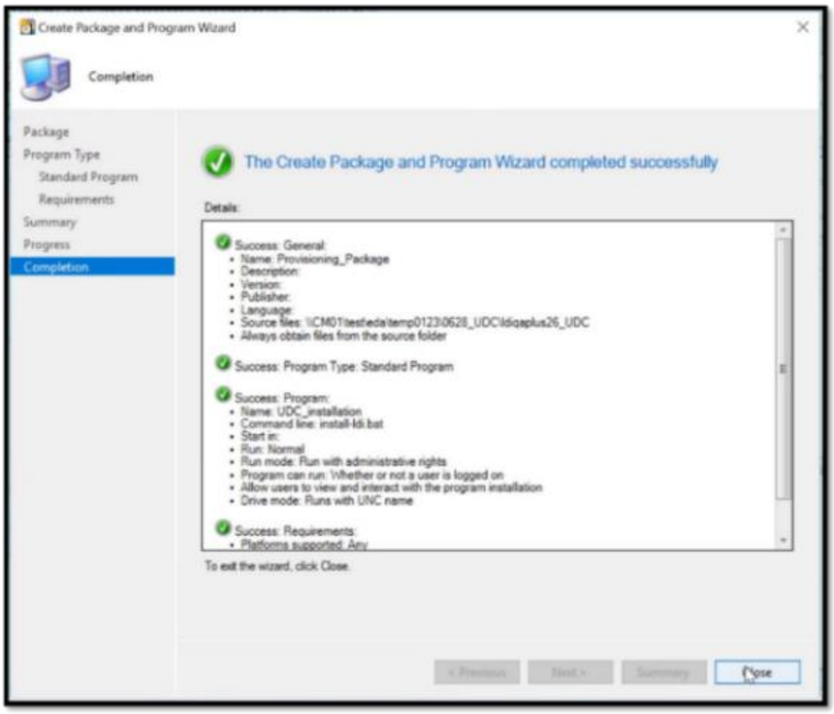
Program Type: Standard Program

Program:
- Name: UDC_installation
- Command line: install-ldi.bat
- Start in:
- Run: Normal
- Run mode: Run with administrative rights
- Program can run: Whether or not a user is logged on
- Allow users to view and interact with the program installation
- Drive mode: Runs with UNC name

Requirements:
- Platforms supported: Any
- Maximum allowed runtime(minutes): 120

To change these settings, click Previous. To apply the settings, click Next.

12. In the **Confirm settings** section, click **Next**, to confirm settings selected for creation of package and program.



The Create Package and Program Wizard completed successfully

Details:

Success: General:
- Name: Provisioning_Package
- Description:
- Version:
- Publisher:
- Language:
- Source files: \\CM01\test\eda\temp01230628_UDC\ldiqaplus26_UDC
- Always obtain files from the source folder

Success: Program Type: Standard Program

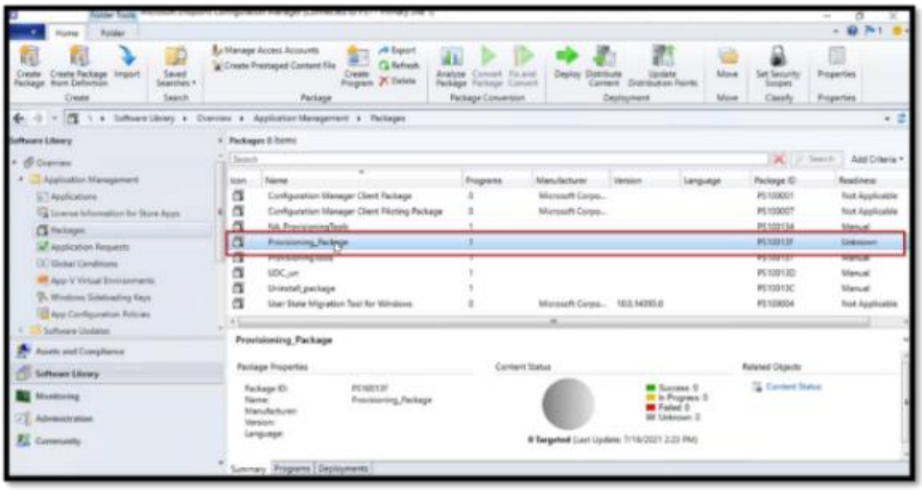
Success: Program:
- Name: UDC_installation
- Command line: install-ldi.bat
- Start in:
- Run: Normal
- Run mode: Run with administrative rights
- Program can run: Whether or not a user is logged on
- Allow users to view and interact with the program installation
- Drive mode: Runs with UNC name

Success: Requirements:
- Platforms supported: Any

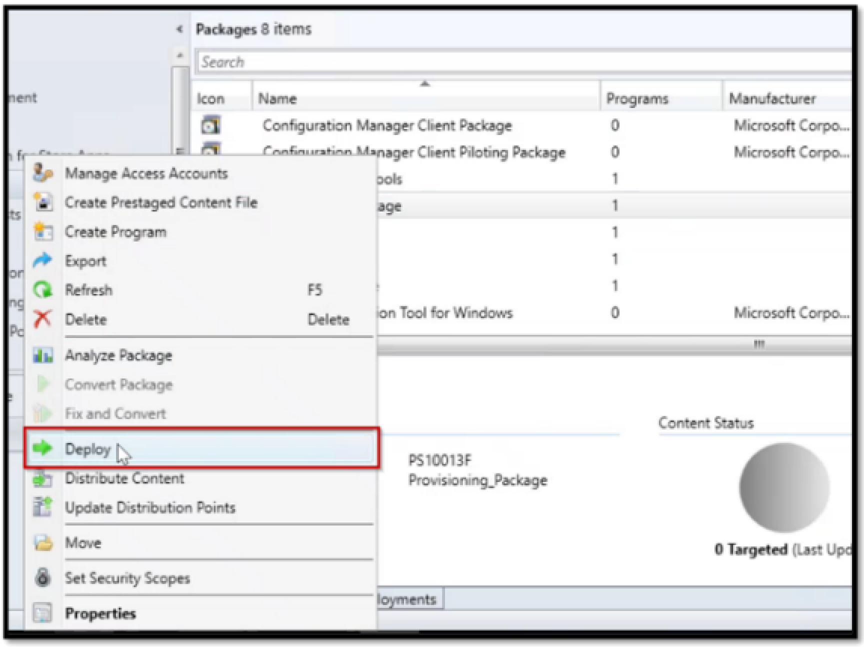
To exit the wizard, click Close.

13. Click **Close** to close the wizard.

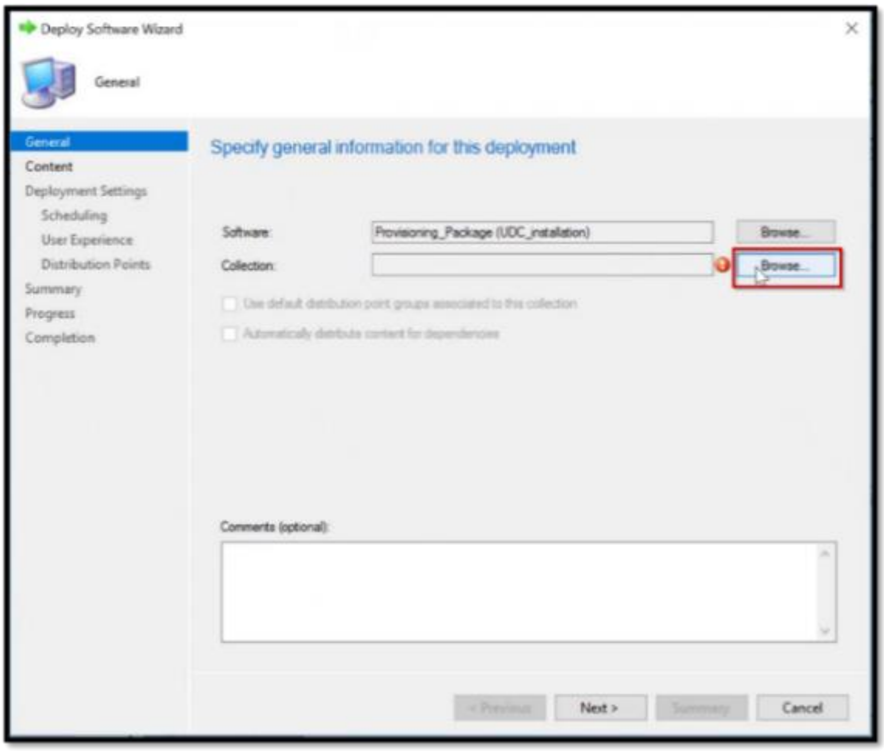
2.2.9.3. Deploy Provisioning Package



14. Select **Packages** in the navigation menu.
15. Right-click on the **package**. For example, Provisioning Package. A pop-up window appears.



16. Click **Deploy**. You see the General section where you can specify the type of deployment.



Specify general information for this deployment

Software: Provisioning_Package (UDC_installation)

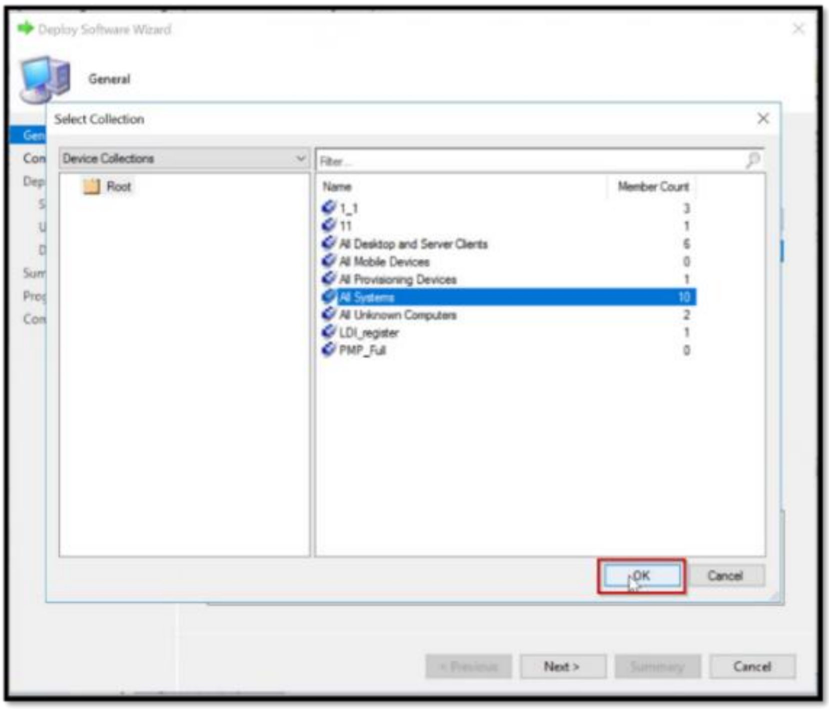
Collection:

□ Use default distribution point groups associated to this collection

□ Automatically distribute content for dependencies

Comments (optional):

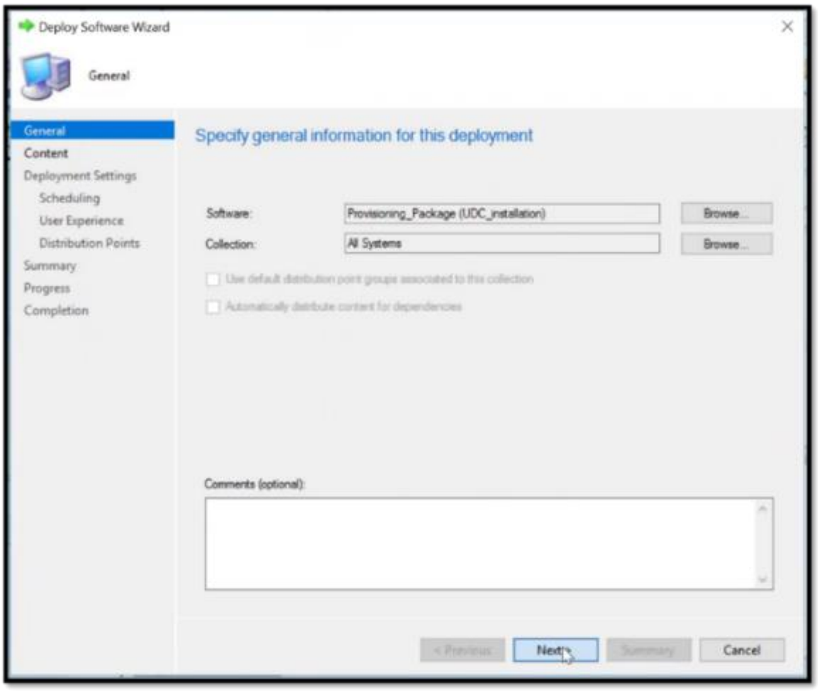
17. In the **Collection** field, click **Browse**. A pop-up window appears.



Name	Member Count
1_1	3
11	1
All Desktop and Server Clients	6
All Mobile Devices	0
All Provisioning Devices	1
All Systems	10
All Unknown Computers	2
LDI_register	1
PMP_Full	0

18. Select an option from the context menu in the pop-up window, e.g., All Systems.

19. Click **OK**.



Deploy Software Wizard

General

Specify general information for this deployment

Software: Provisioning_Package (UDC_installation)

Collection: All Systems

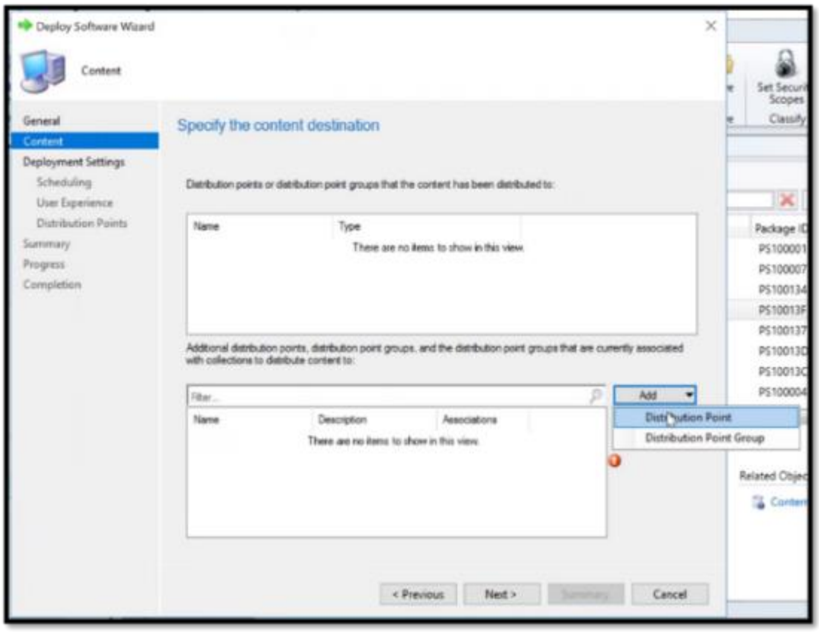
□ Use default distribution point groups associated to this collection

□ Automatically distribute content for dependencies

Comments (optional):

20. Click **Next**. The **Content** section appears.

2.2.9.4. Specify Content Destination



Deploy Software Wizard

Content

Specify the content destination

Distribution points or distribution point groups that the content has been distributed to:

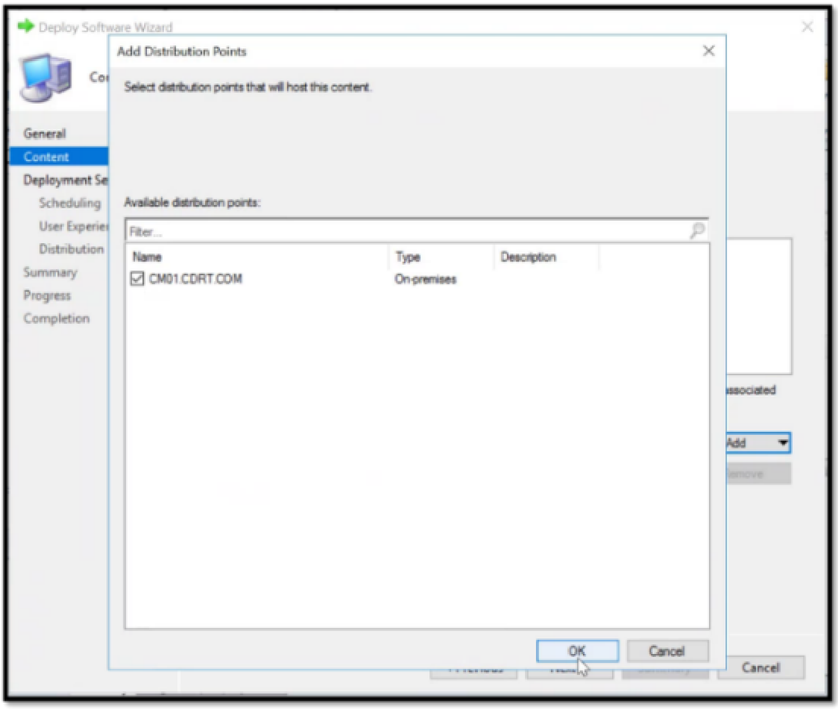
Name	Type
There are no items to show in this view.	

Additional distribution points, distribution point groups, and the distribution point groups that are currently associated with collections to distribute content to:

Name	Description	Associations
There are no items to show in this view.		

21. Click **Add** to view a drop-down menu.

22. Click **Distribution Point**. A pop-up window appears.



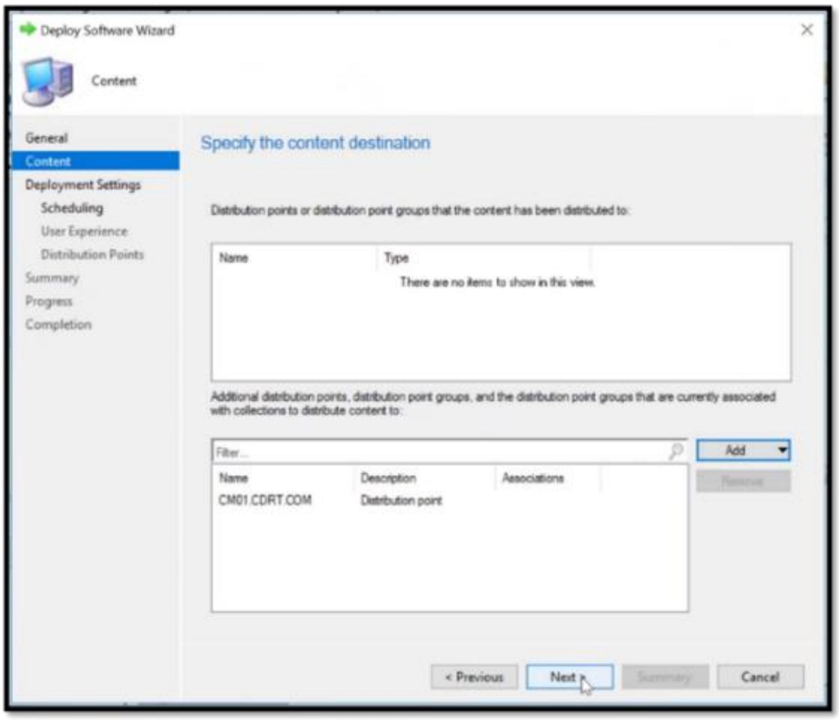
Select distribution points that will host this content.

Available distribution points:

Name	Type	Description
☑ CM01.CDRT.COM	On-premises	

23. Select the **CM01.CDRT.COM** checkbox.

24. Click **OK**.



Specify the content destination

Distribution points or distribution point groups that the content has been distributed to:

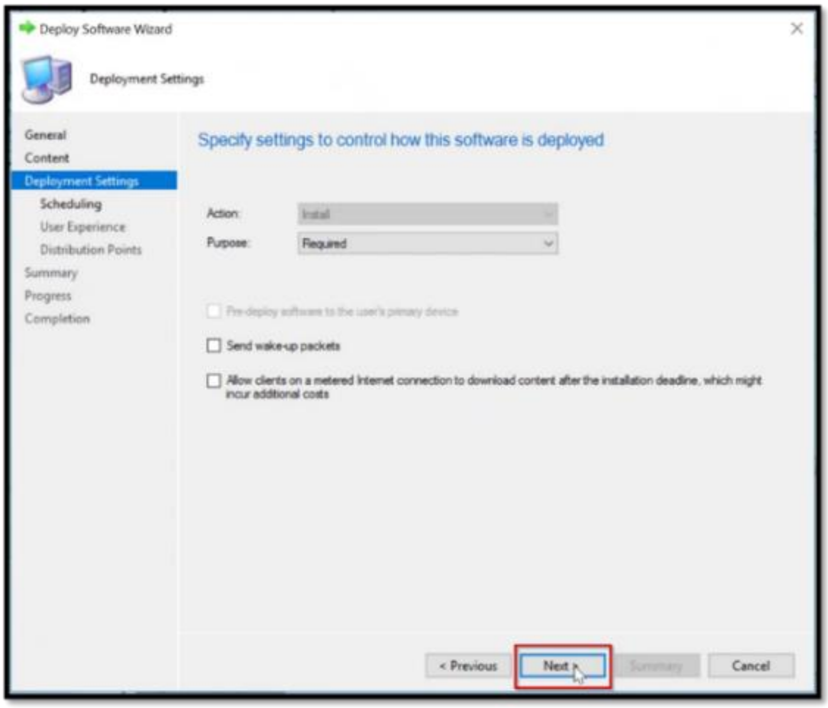
Name	Type
	There are no items to show in this view.

Additional distribution points, distribution point groups, and the distribution point groups that are currently associated with collections to distribute content to:

Name	Description	Associations
CM01.CDRT.COM	Distribution point	

25. Click **Next**. The **Deployment Settings** section appears.

2.2.9.5. Deployment Settings



Specify settings to control how this software is deployed

Action: Install

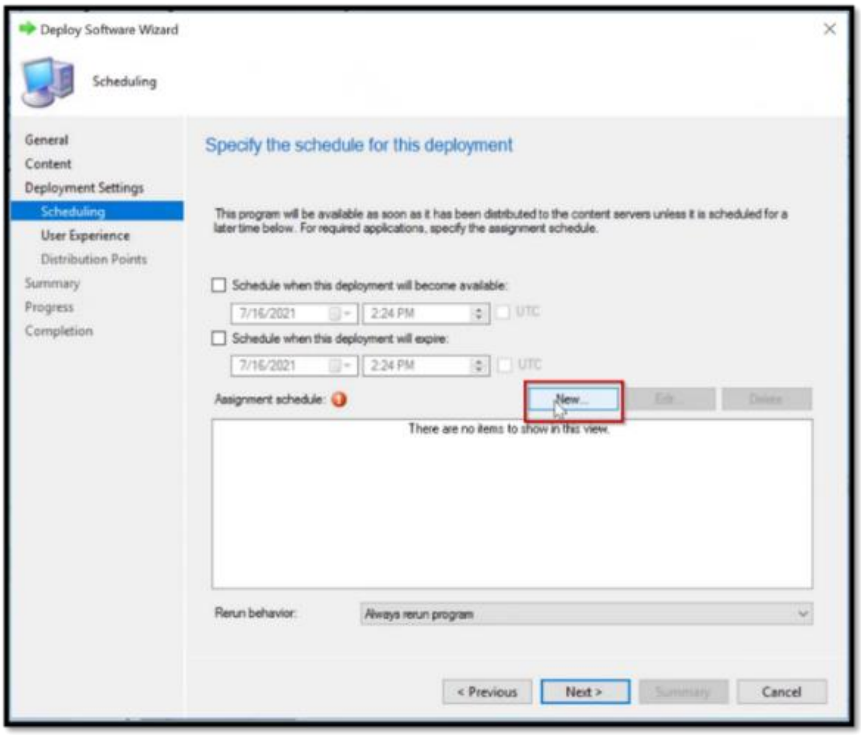
Purpose: Required

□ Pre-deploy software to the user's primary device

□ Send wake-up packets

□ Allow clients on a metered Internet connection to download content after the installation deadline, which might incur additional costs

26. In the **Purpose** field, select **Required**.
27. Click **Next**. The Scheduling section appears.



Specify the schedule for this deployment

This program will be available as soon as it has been distributed to the content servers unless it is scheduled for a later time below. For required applications, specify the assignment schedule.

□ Schedule when this deployment will become available:

7/16/2021 2:24 PM □ UTC

□ Schedule when this deployment will expire:

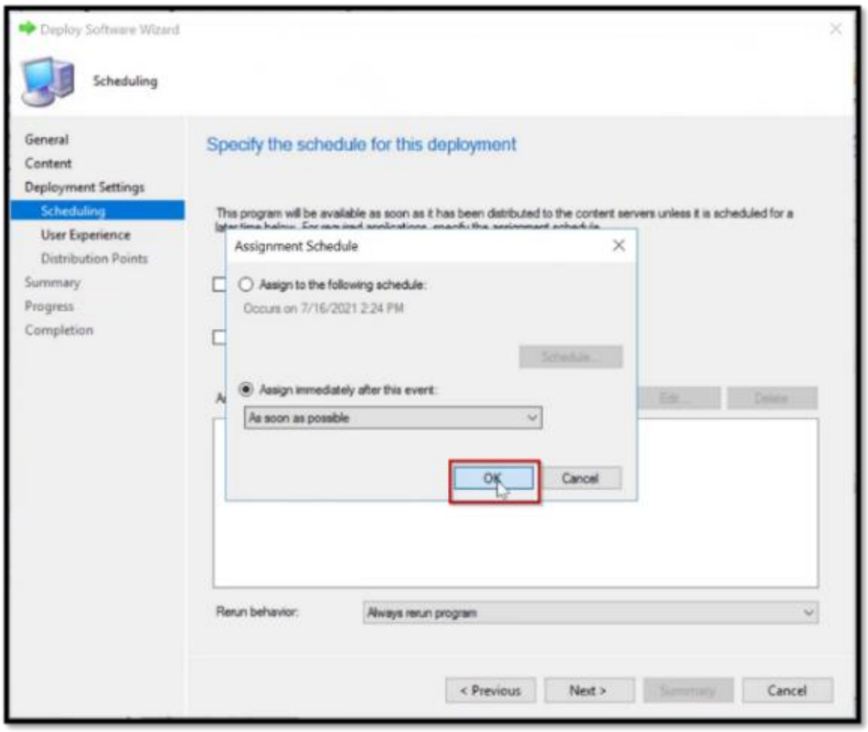
7/16/2021 2:24 PM □ UTC

Assignment schedule:

There are no items to show in this view.

Rerun behavior: Always rerun program

28. Click New. The Deploy Software Wizard appears.



Specify the schedule for this deployment

This program will be available as soon as it has been distributed to the content servers unless it is scheduled for a later time below. For required applications, specify the assignment schedule.

Assignment Schedule

○ Assign to the following schedule:

Occurs on 7/16/2021 2:24 PM

● Assign immediately after this event:

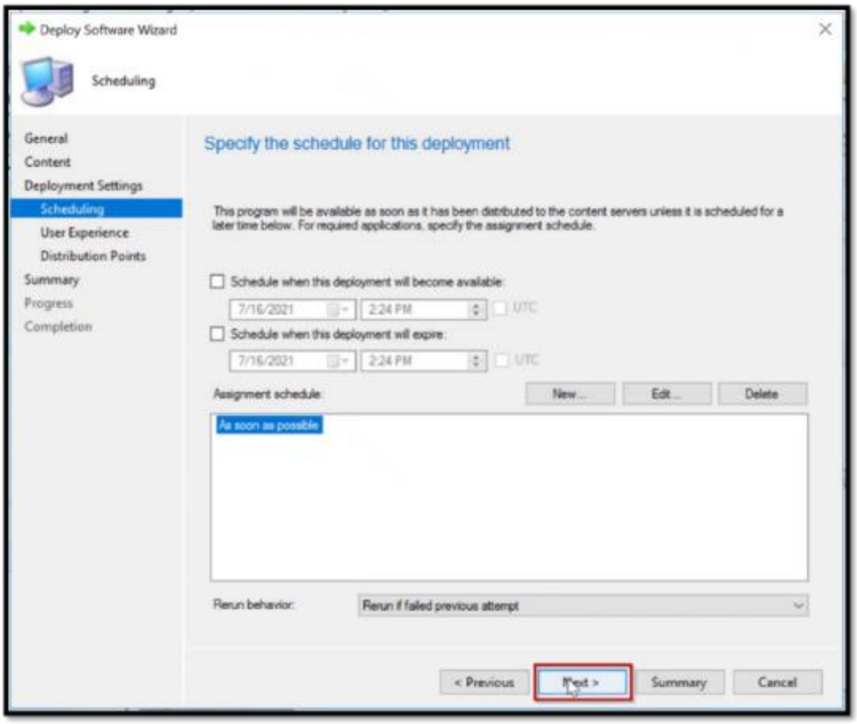
As soon as possible

Rerun behavior: Always rerun program

29. Select Assign immediately after this event.

30. Select **As soon as possible** from the drop-down list.

31. Click **OK**.



Specify the schedule for this deployment

This program will be available as soon as it has been distributed to the content servers unless it is scheduled for a later time below. For required applications, specify the assignment schedule.

☐ Schedule when this deployment will become available:

7/16/2021 2:24 PM ☐ UTC

☐ Schedule when this deployment will expire:

7/16/2021 2:24 PM ☐ UTC

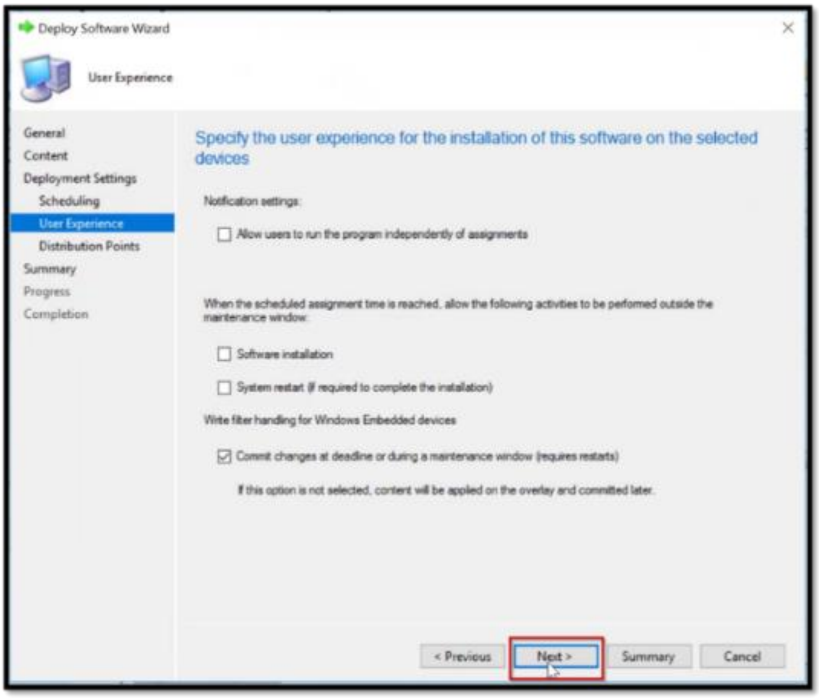
Assignment schedule:

As soon as possible

Rerun behavior: Rerun if failed previous attempt

32. Click **Next**.

2.2.9.6. User Experience



Specify the user experience for the installation of this software on the selected devices

Notification settings:

□ Allow users to run the program independently of assignments

When the scheduled assignment time is reached, allow the following activities to be performed outside the maintenance window:

□ Software installation

□ System restart (if required to complete the installation)

Write filter handling for Windows Embedded devices

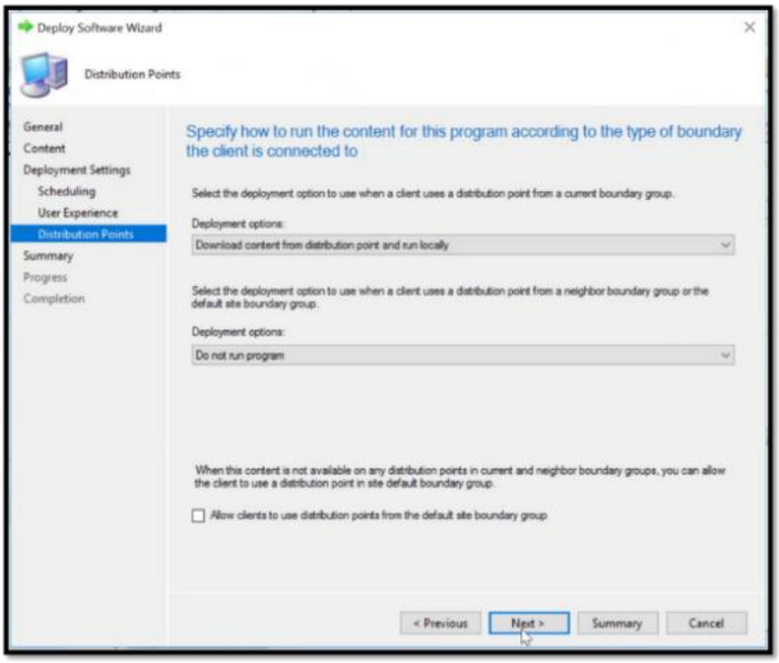
☑ Commit changes at deadline or during a maintenance window (requires restarts)

If this option is not selected, content will be applied on the overlay and committed later.

Keep user experience settings as default settings.

33. Click **Next.** You see the **Distribution Points** section.

2.2.9.7. Distributions Points



Specify how to run the content for this program according to the type of boundary the client is connected to

Select the deployment option to use when a client uses a distribution point from a current boundary group.

Deployment options: Download content from distribution point and run locally

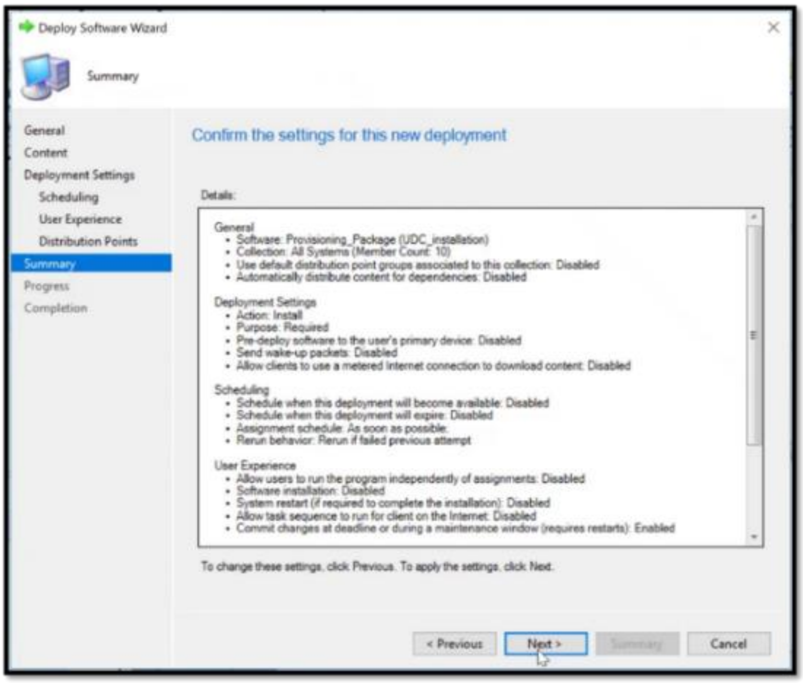
Select the deployment option to use when a client uses a distribution point from a neighbor boundary group or the default site boundary group.

Deployment options: Do not run program

When this content is not available on any distribution points in current and neighbor boundary groups, you can allow the client to use a distribution point in site default boundary group.

□ Allow clients to use distribution points from the default site boundary group

34. Keep the Distribution Points settings as the default settings and click **Next.**



Confirm the settings for this new deployment

Details:

General
- Software: Provisioning_Package (UDC_installation)
- Collection: All Systems (Member Count: 10)
- Use default distribution point groups associated to this collection: Disabled
- Automatically distribute content for dependencies: Disabled

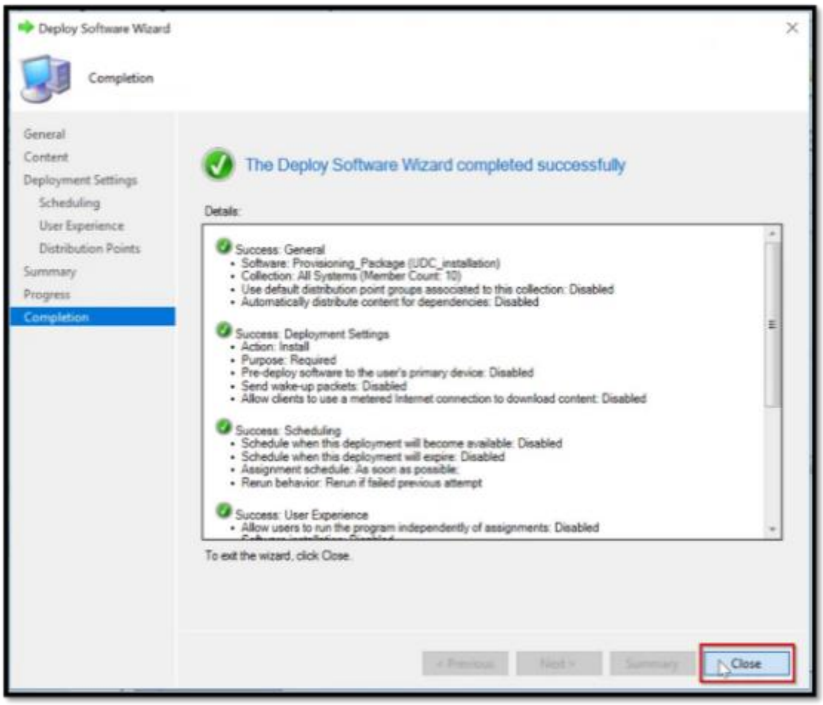
Deployment Settings
- Action: Install
- Purpose: Required
- Pre-deploy software to the user's primary device: Disabled
- Send wake-up packets: Disabled
- Allow clients to use a metered Internet connection to download content: Disabled

Scheduling
- Schedule when this deployment will become available: Disabled
- Schedule when this deployment will expire: Disabled
- Assignment schedule: As soon as possible
- Rerun behavior: Rerun if failed previous attempt

User Experience
- Allow users to run the program independently of assignments: Disabled
- Software installation: Disabled
- System restart (if required to complete the installation): Disabled
- Allow task sequence to run for client on the Internet: Disabled
- Commit changes at deadline or during a maintenance window (requires restarts): Enabled

To change these settings, click Previous. To apply the settings, click Next.

35. Click **Next** to confirm General, Deployment, Scheduling and User Experience settings.



The Deploy Software Wizard completed successfully

Details:

Success: General
- Software: Provisioning_Package (UDC_installation)
- Collection: All Systems (Member Count: 10)
- Use default distribution point groups associated to this collection: Disabled
- Automatically distribute content for dependencies: Disabled

Success: Deployment Settings
- Action: Install
- Purpose: Required
- Pre-deploy software to the user's primary device: Disabled
- Send wake-up packets: Disabled
- Allow clients to use a metered Internet connection to download content: Disabled

Success: Scheduling
- Schedule when this deployment will become available: Disabled
- Schedule when this deployment will expire: Disabled
- Assignment schedule: As soon as possible
- Rerun behavior: Rerun if failed previous attempt

Success: User Experience
- Allow users to run the program independently of assignments: Disabled

To exit the wizard, click Close.

36. Click **Close** to exit the wizard.

2.2.9.8. Deploy LDI Windows (Virtual) Package via SCCM

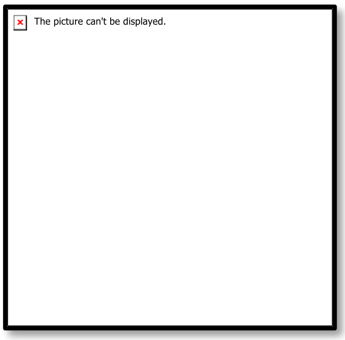
The process of deployment of LDI Windows (Virtual) Package is same as the standard agent deployment process.

Refer to Configure SCCM to Deploy LDI Windows (Physical) Package on the Devices in the Application Mode for deploying LDI Windows (Virtual) Package in the Application Mode.

Refer to Configure SCCM to Deploy LDI Windows (Physical) Package on the Devices in the Package Mode for deploying LDI Windows (Virtual) Package in the Package Mode.

Note: In the **Detection Rule** window:

- If the Setting Type is **File System**, enter **SysTrack** in the File or Folder name to check if the LDI Windows (Virtual) Agent is installed.

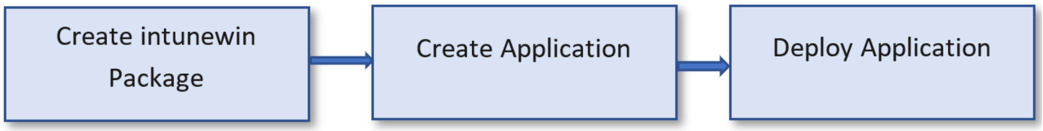


- If the Setting Type is **Registry**, enter SOFTWARE\WOW6432Node\Lakeside Software\LsiAgent\Debug to check if LDI windows (Virtual) Agent is installed.

2.3 Microsoft InTune

This chapter allows you to enroll your device in LDI using Microsoft InTune. For this, it provides you an overview of steps to follow to enroll devices.

Note: You must have an Azure Active Directory (AAD) account to enroll your device in InTune.



2.3.1 Purpose

You can configure Microsoft InTune to install the LDI Provisioning Package on all the devices in your organization and register them as per Service License Agreement between your organization and LDI Solutions. Instead of downloading Provisioning package on each device you can use Microsoft InTune to run it on the entire fleet of device. This saves your time and effort.

2.3.2 Prerequisite

Download the LDI Provisioning Package on the device you want to configure Microsoft InTune onto and deploy the package on the entire fleet of devices in your organization. Refer to Onboard your fleet to download and install he package.

2.3.3 Configure Microsoft InTune to Deploy LDI Provisioning Package

LDI agent is distributed as a single exe InnoSetup file or as a zip archive with Universal Device Client (UDC) agent and jwt client. Once you create the .intunewin package, you can upload and deploy/assign the application using InTune console.

2.3.4 Create .intunewin Package

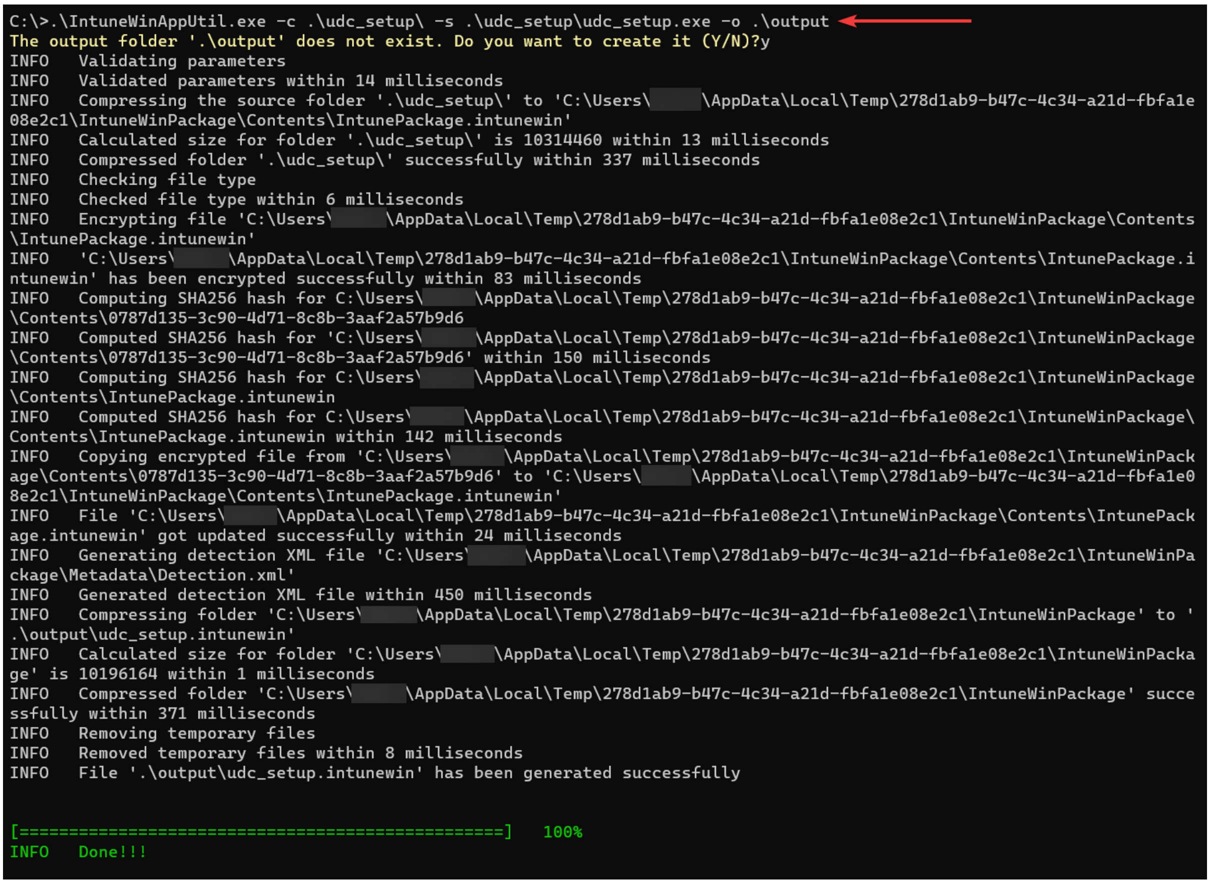
1. Log in to LDI.
2. Select **Help & Resources → Instructions & Agents**.
3. From the **Select System** drop-down list, select **Windows (Physical).**
4. For the onboarding method, select **Microsoft Intune**.
5. Click **Confirm**.

Note: If you're not connected to the Azure ID, select Organization Settings → Connectors to set the values of Directory (Tenant) ID, Application (Client) ID, and App Secret fields.

6. In the **Instructions for Windows Intune Devices Onboarding** page, select the permissions. Refer Provide a Permission.
7. Click **Next**.
8. Select **Maximum Usage** and **Installer Expiration** values from the respective drop-downs.
9. Click **Download**.
10. Upload the .intunewin into Applications.
11. Enter the application ID from the Intune URL in the **Application ID** field. Refer Register an Application to get the Application ID.

12. Unzip the udc_setup.exe file.
13. Convert exe file into .intunewin package. Create a new folder and copy the received installer file in that folder. Then, install and run IntuneWinAppUtil tool with the following parameters: IntuneWinAppUtil -c <created input folder with exe file> -s <exe installer> -o <output_folder>. This command generates .intunewin file in the output folder. For example:

.\IntuneWinAppUtil.exe -c .\udc_setup\ -s .\udc_setup\udc_setup.exe -o .\output

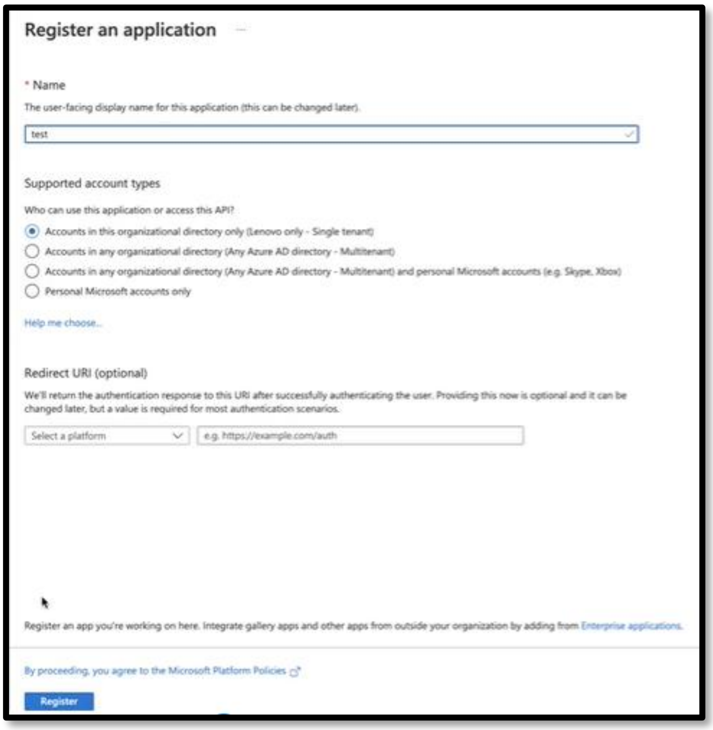


```
C:\>.\IntuneWinAppUtil.exe -c .\udc_setup\ -s .\udc_setup\udc_setup.exe -o .\output
The output folder '.\output' does not exist. Do you want to create it (Y/N)?y
INFO   Validating parameters
INFO   Validated parameters within 14 milliseconds
INFO   Compressing the source folder '.\udc_setup\' to 'C:\Users\[redacted]\AppData\Local\Temp\278d1ab9-b47c-4c34-a21d-fbfa1e
08e2c1\IntuneWinPackage\Contents\IntunePackage.intunewin'
INFO   Calculated size for folder '.\udc_setup\' is 10314460 within 13 milliseconds
INFO   Compressed folder '.\udc_setup\' successfully within 337 milliseconds
INFO   Checking file type
INFO   Checked file type within 6 milliseconds
INFO   Encrypting file 'C:\Users\[redacted]\AppData\Local\Temp\278d1ab9-b47c-4c34-a21d-fbfa1e08e2c1\IntuneWinPackage\Contents
\IntunePackage.intunewin'
INFO   'C:\Users\[redacted]\AppData\Local\Temp\278d1ab9-b47c-4c34-a21d-fbfa1e08e2c1\IntuneWinPackage\Contents\IntunePackage.i
ntunewin' has been encrypted successfully within 83 milliseconds
INFO   Computing SHA256 hash for C:\Users\[redacted]\AppData\Local\Temp\278d1ab9-b47c-4c34-a21d-fbfa1e08e2c1\IntuneWinPackage
\Contents\0787d135-3c90-4d71-8c8b-3aaf2a57b9d6
INFO   Computed SHA256 hash for 'C:\Users\[redacted]\AppData\Local\Temp\278d1ab9-b47c-4c34-a21d-fbfa1e08e2c1\IntuneWinPackage
\Contents\0787d135-3c90-4d71-8c8b-3aaf2a57b9d6' within 150 milliseconds
INFO   Computing SHA256 hash for C:\Users\[redacted]\AppData\Local\Temp\278d1ab9-b47c-4c34-a21d-fbfa1e08e2c1\IntuneWinPackage
\Contents\IntunePackage.intunewin
INFO   Computed SHA256 hash for C:\Users\[redacted]\AppData\Local\Temp\278d1ab9-b47c-4c34-a21d-fbfa1e08e2c1\IntuneWinPackage\
Contents\IntunePackage.intunewin within 142 milliseconds
INFO   Copying encrypted file from 'C:\Users\[redacted]\AppData\Local\Temp\278d1ab9-b47c-4c34-a21d-fbfa1e08e2c1\IntuneWinPack
age\Contents\0787d135-3c90-4d71-8c8b-3aaf2a57b9d6' to 'C:\Users\[redacted]\AppData\Local\Temp\278d1ab9-b47c-4c34-a21d-fbfa1e0
8e2c1\IntuneWinPackage\Contents\IntunePackage.intunewin'
INFO   File 'C:\Users\[redacted]\AppData\Local\Temp\278d1ab9-b47c-4c34-a21d-fbfa1e08e2c1\IntuneWinPackage\Contents\IntunePack
age.intunewin' got updated successfully within 24 milliseconds
INFO   Generating detection XML file 'C:\Users\[redacted]\AppData\Local\Temp\278d1ab9-b47c-4c34-a21d-fbfa1e08e2c1\IntuneWinPa
ckage\Metadata\Detection.xml'
INFO   Generated detection XML file within 450 milliseconds
INFO   Compressing folder 'C:\Users\[redacted]\AppData\Local\Temp\278d1ab9-b47c-4c34-a21d-fbfa1e08e2c1\IntuneWinPackage' to '
.\output\udc_setup.intunewin'
INFO   Calculated size for folder 'C:\Users\[redacted]\AppData\Local\Temp\278d1ab9-b47c-4c34-a21d-fbfa1e08e2c1\IntuneWinPacka
ge' is 10196164 within 1 milliseconds
INFO   Compressed folder 'C:\Users\[redacted]\AppData\Local\Temp\278d1ab9-b47c-4c34-a21d-fbfa1e08e2c1\IntuneWinPackage' succe
ssfully within 371 milliseconds
INFO   Removing temporary files
INFO   Removed temporary files within 8 milliseconds
INFO   File '.\output\udc_setup.intunewin' has been generated successfully


[=================================================]   100%
INFO   Done!!!
```

2.3.5 Register an Application

1. Open Manage Azure Active Directory.
2. Select **App Registrations**.
3. Click **New Registration**.



Register an application

* Name

The user-facing display name for this application (this can be changed later).

test

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Lenovo only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform | e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

By proceeding, you agree to the Microsoft Platform Policies

4. Enter a name for the application and click **Register**. The Application ID and the Directory ID are created.

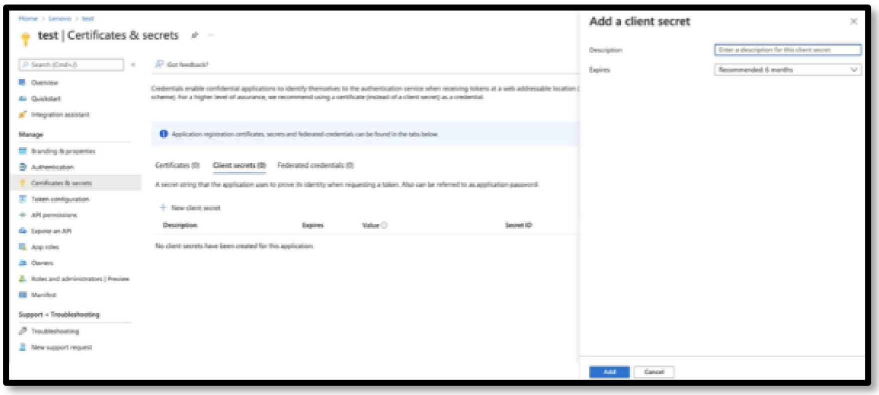
2.3.6 Provide a Permission

You need to provide certain permissions to an application to work with InTune.

Note: Before providing permissions, you need to create a secret ID.

To create a secret ID

1. Register an Application.
2. Click **Certificates & Secrets**.



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) | Client secrets (0) | Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID

No client secrets have been created for this application.

Add a client secret

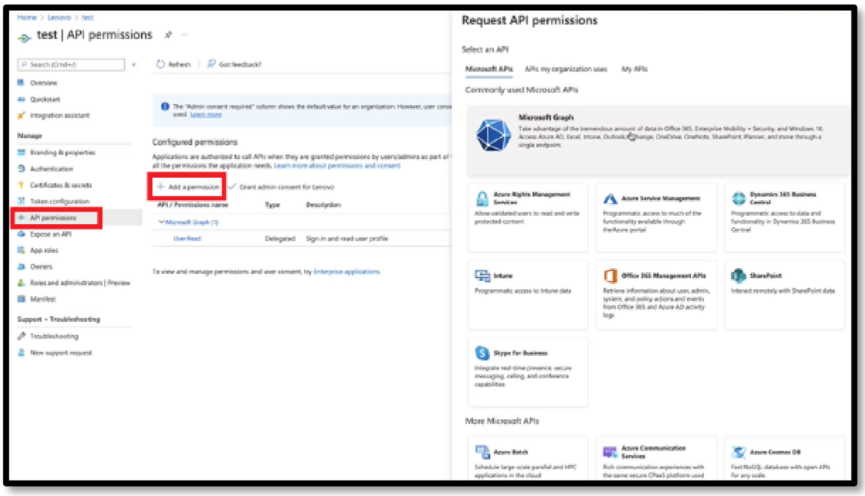
Description: Enter a description for this client secret

Expires: Recommended: 6 months

3. Enter a secret ID in the **Description** field and click **Add**.

To provide a permission

1. Click **API Permissions** and then click **Add a permission**.



The "Admin consent required" column shows the default value for an organization. However, user conse[nt can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be] used. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of [the consent process. The list of configured permissions should include] all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description
⌄Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile

To view and manage permissions and user consent, try Enterprise applications.

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Rights Management Services
Allow validated users to read and write protected content

Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Dynamics 365 Business Central
Programmatic access to data and functionality in Dynamics 365 Business Central

Intune
Programmatic access to Intune data

Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity logs

SharePoint
Interact remotely with SharePoint data

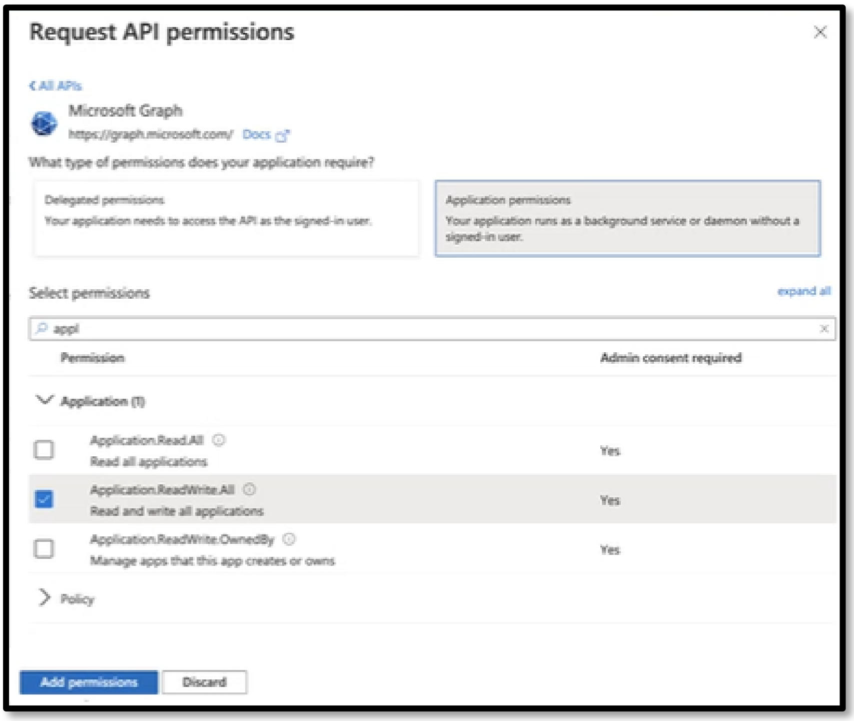
Skype for Business
Integrate real-time presence, secure messaging, calling, and conference capabilities

Azure Batch
Schedule large-scale parallel and HPC applications in the cloud

Azure Communication Services
Rich communication experiences with the same secure CPaaS platform used

Azure Cosmos DB
Fast NoSQL database with open APIs for any scale.

2. Select **Microsoft Graph** and then select **Application permissions.** The **Select permissions** window appears.



Microsoft Graph
https://graph.microsoft.com/

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

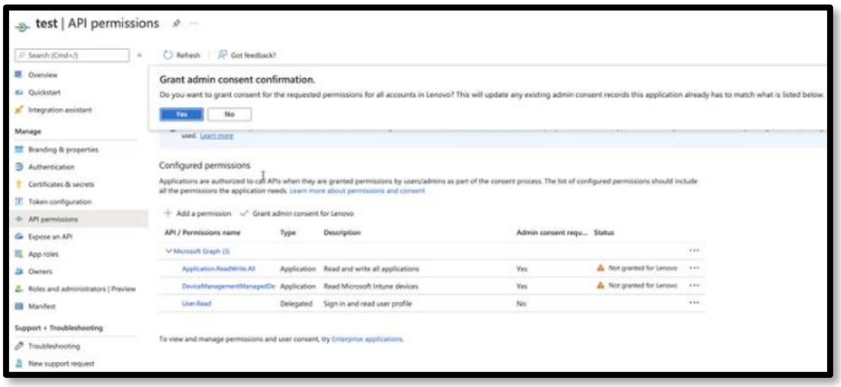
Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

appl

	Permission	Admin consent required
	⌄ Application (1)	
□	Application.Read.All Read all applications	Yes
☑	Application.ReadWrite.All Read and write all applications	Yes
□	Application.ReadWrite.OwnedBy Manage apps that this app creates or owns	Yes
	› Policy	

3. Search for the required permissions, select the respective check boxes, and then click **Add permissions**.



Grant admin consent confirmation.

Do you want to grant consent for the requested permissions for all accounts in Lenovo? This will update any existing admin consent records this application already has to match what is listed below.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

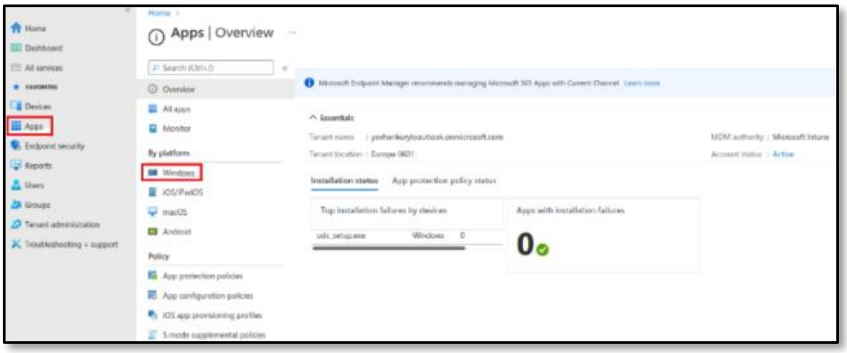
API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
Application.ReadWrite.All	Application	Read and write all applications	Yes	Not granted for Lenovo
DeviceManagementManagedDe	Application	Read Microsoft Intune devices	Yes	Not granted for Lenovo
User.Read	Delegated	Sign in and read user profile	No	

To view and manage permissions and user consent, try Enterprise applications.

4. Click **Grant admin consent for Lenovo**. The **Grant admin consent confirmation** window appears.
5. Click **Yes**.

2.3.7 Create and Add Windows Application to InTune

1. Log in to InTune console and select **Apps**, then select **Windows** platform.



Microsoft Endpoint Manager recommends managing Microsoft 365 Apps with Current Channel. Learn more

Tenant location : Europe 0601

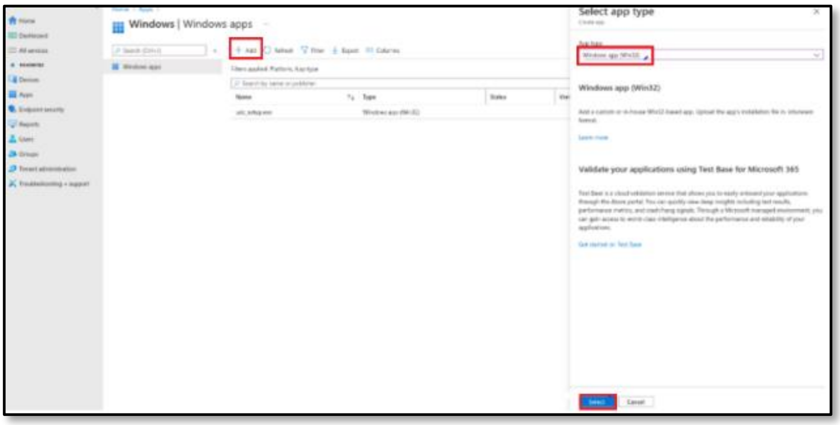
MDM authority : Microsoft Intune

Account status : Active

udc_setup.exe Windows 0

0

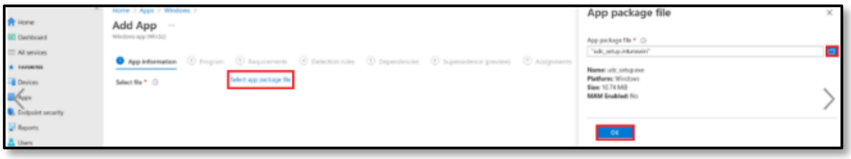
2. Click **Add** and select **Windows app (Win32) App** type, and then click **Select**.



Windows app (Win32)

Validate your applications using Test Base for Microsoft 365

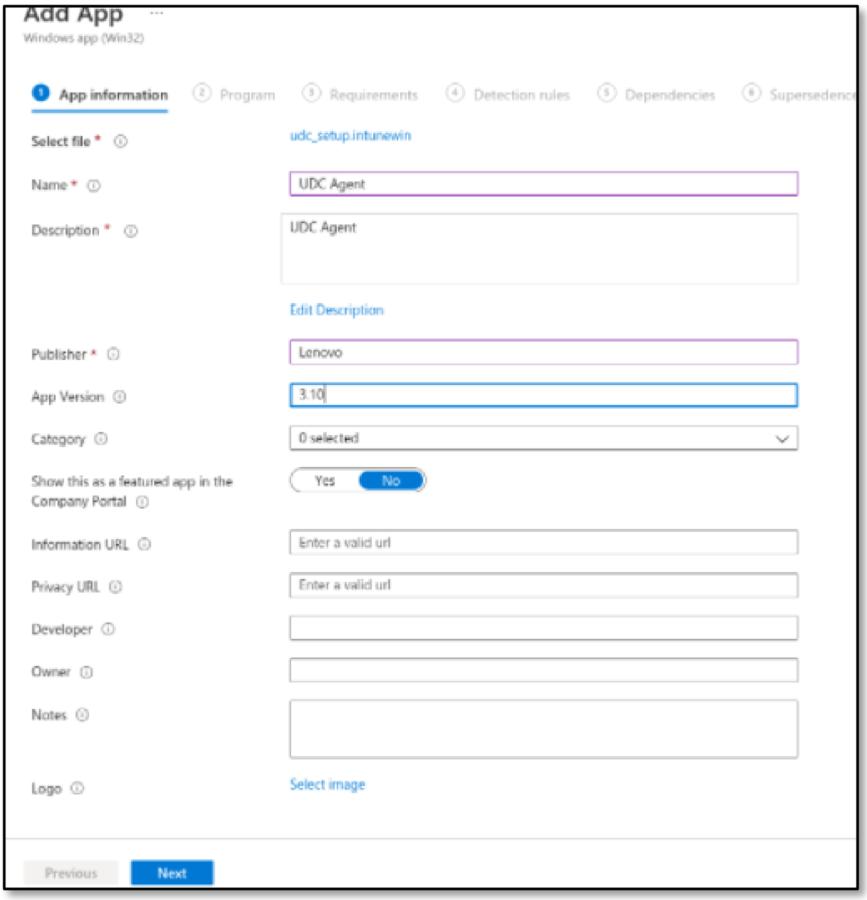
3. Select **.intunewin package file**.



"udc_setup.intunewin"

Name: udc_setup.exe
Platform: Windows
Size: 10.74 MB
MAM Enabled: No

4. Provide required app information.



Add App ···

Windows app (Win32)

Select file * udc_setup.intunewin

Name * UDC Agent

Description * UDC Agent

Publisher * Lenovo

App Version 3.10

Category 0 selected

Show this as a featured app in the Company Portal Yes [✓ No]

Information URL Enter a valid url

Privacy URL Enter a valid url

Developer

Owner

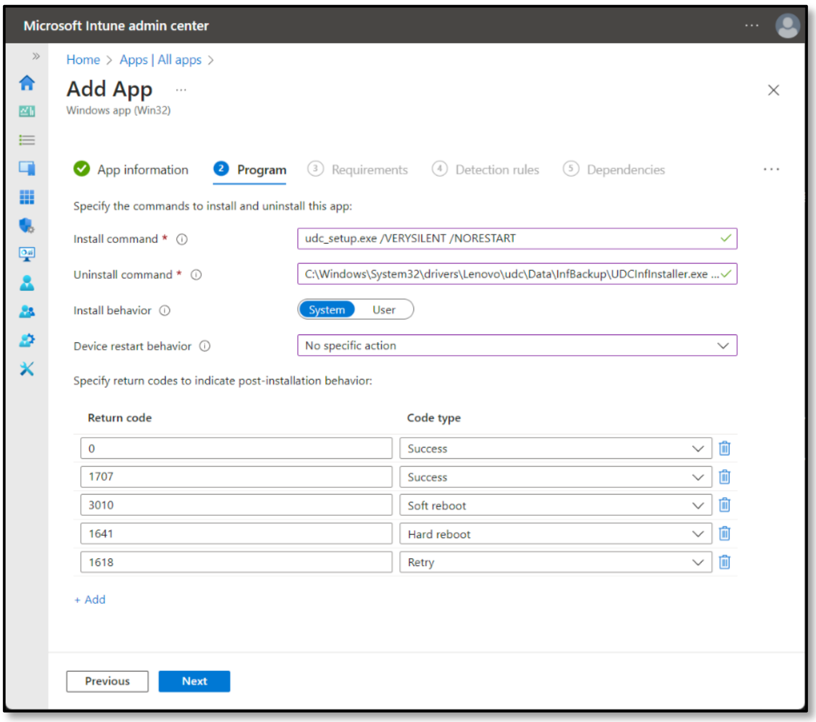
Notes

Logo

5. Provide application install and uninstall commands.

   Install command: udc_setup.exe /VERYSILENT /NORESTART

Uninstall command: C:\Windows\System32\drivers\Lenovo\udc\Data\InfBackup\UDCInfInstaller.exe -uninstall



Specify the commands to install and uninstall this app:

Install command *: udc_setup.exe /VERYSILENT /NORESTART

Uninstall command *: C:\Windows\System32\drivers\Lenovo\udc\Data\InfBackup\UDCInfInstaller.exe ...

Install behavior: ● System ○ User

Device restart behavior: No specific action

Specify return codes to indicate post-installation behavior:

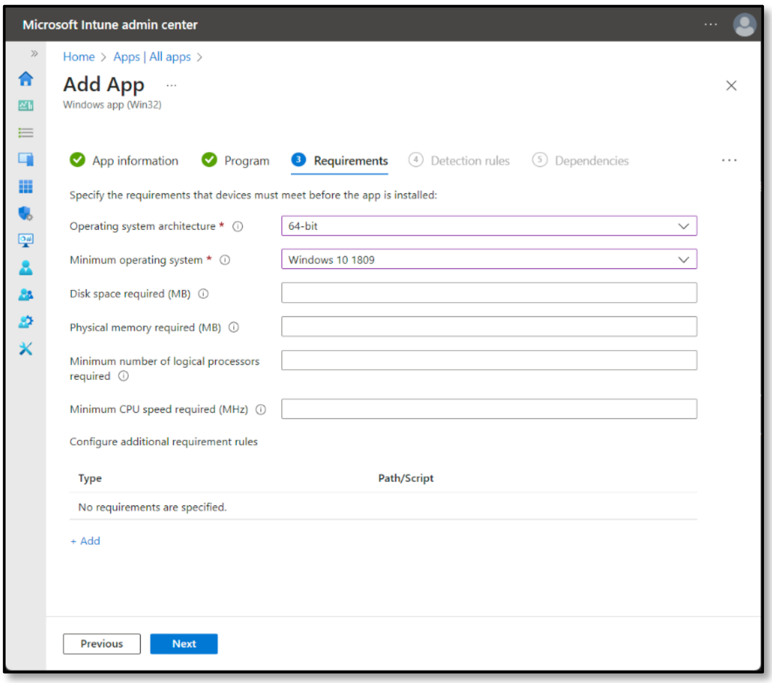
Return code	Code type
0	Success
1707	Success
3010	Soft reboot
1641	Hard reboot
1618	Retry

+ Add

6. Provide requirements for the application.

Note:

- Operating system architecture requirement is 64-bit. Minimum operating system is Windows 10 1809.
- You can also provide optional requirements such as disc space, number of processors, etc.



Specify the requirements that devices must meet before the app is installed:

Operating system architecture *: 64-bit

Minimum operating system *: Windows 10 1809

Disk space required (MB):

Physical memory required (MB):

Minimum number of logical processors required:

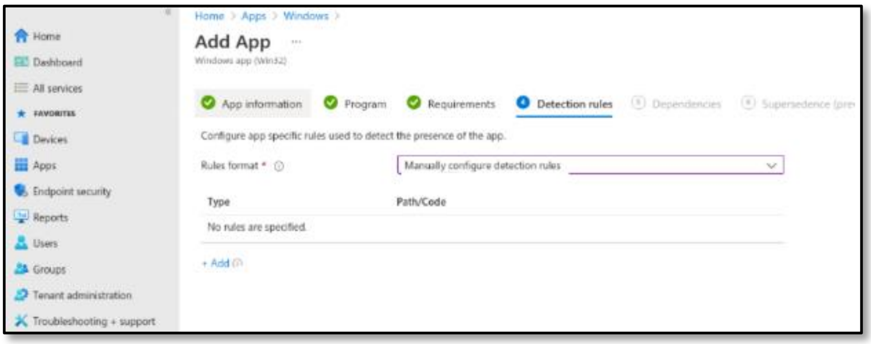
Minimum CPU speed required (MHz):

Configure additional requirement rules

Type	Path/Script
No requirements are specified.	

+ Add

7. Select a detection rule from the **Rules format** drop-down list. These rules allow you to detect if application is installed or not. You can select manually configured rules or custom detection script.



Add App

Windows app (Win32)

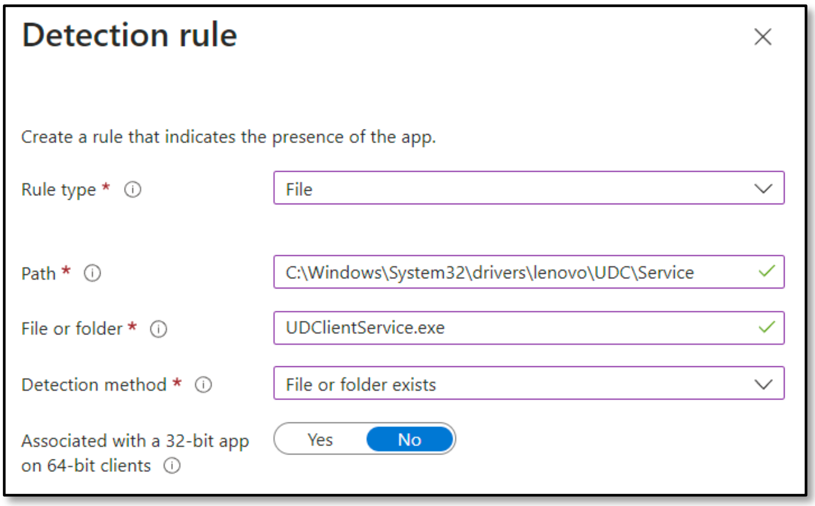
Configure app specific rules used to detect the presence of the app.

Rules format * : Manually configure detection rules

Type	Path/Code
No rules are specified.	

Note: The following are manually detection rules:

- **MSI** - Detects by MSI product code
- **File** - This rule allows to detect app based on filesystem information: file or folder exists, created/modified date, file size
- **Registry** - The rule allows to detect app based on registry information: key exists, key doesn't exist, value comparison



Detection rule

Create a rule that indicates the presence of the app.

Rule type * : File

Path * : C:\Windows\System32\drivers\lenovo\UDC\Service

File or folder * : UDClientService.exe

Detection method * : File or folder exists

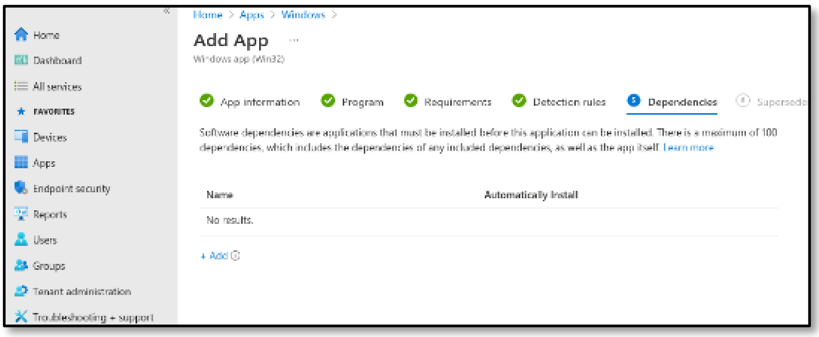
Associated with a 32-bit app on 64-bit clients: Yes [✓ No]

Note: UDC agent is installed as a driver to
Path: C:\Windows\System32\drivers\Lenovo\udc\Service.

File: UDClientService.exe

Detection method: File or folder exists

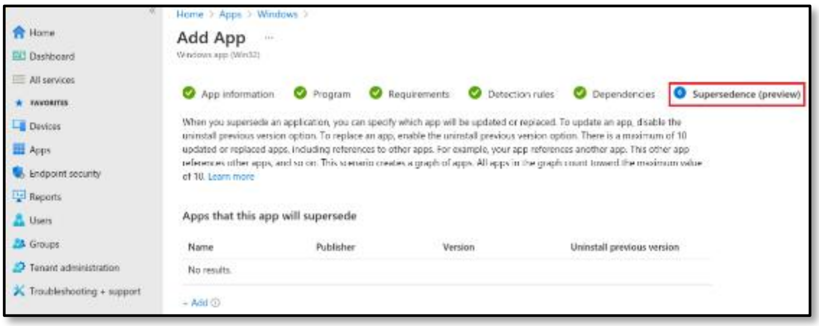
Optional Step 1: Click **Dependencies**, if required.



Software dependencies are applications that must be installed before this application can be installed. There is a maximum of 100 dependencies, which includes the dependencies of any included dependencies, as well as the app itself. Learn more

Name	Automatically Install
No results.	

Optional Step 2: Click **Supersedence**, if required.

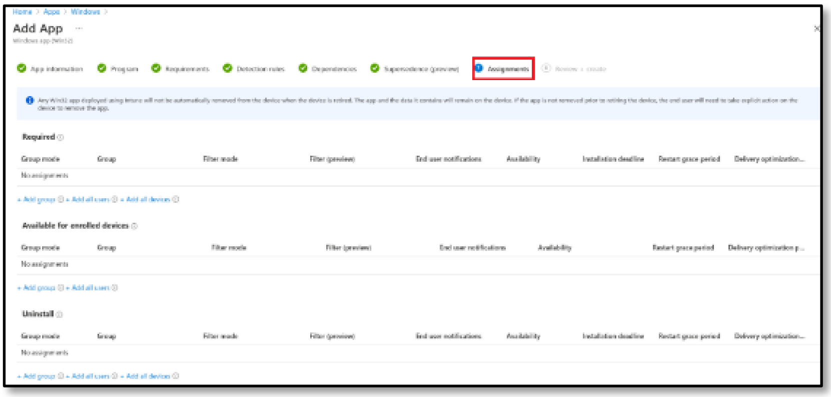


When you supersede an application, you can specify which app will be updated or replaced. To update an app, disable the uninstall previous version option. To replace an app, enable the uninstall previous version option. There is a maximum of 10 updated or replaced apps, including references to other apps. For example, your app references another app. This other app references other apps, and so on. This scenario creates a graph of apps. All apps in the graph count toward the maximum value of 10. Learn more

Apps that this app will supersede

Name	Publisher	Version	Uninstall previous version
No results.			

Optional Step 3: Click **Assignments** to deploy the application to the selected device or a group of devices. You can skip this step for creating an application.



Any Win32 app deployed using Intune will not be automatically removed from the device when the device is retired. The app and the data it contains will remain on the device. If the app is not removed prior to retiring the device, the end user will need to take explicit action on the device to remove the app.

Required

Group mode	Group	Filter mode	Filter (preview)	End user notifications	Availability	Installation deadline	Restart grace period	Delivery optimization...
No assignments								

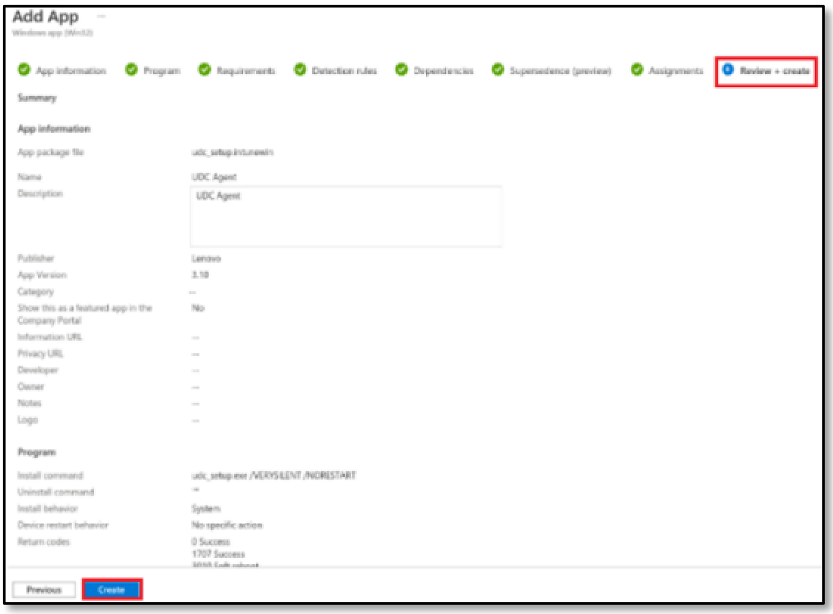
Available for enrolled devices

Group mode	Group	Filter mode	Filter (preview)	End user notifications	Availability	Restart grace period	Delivery optimization p...
No assignments							

Uninstall

Group mode	Group	Filter mode	Filter (preview)	End user notifications	Availability	Installation deadline	Restart grace period	Delivery optimization...
No assignments								

8. Click **Review + create**. If the review summary is correct, click **Create**.



Summary

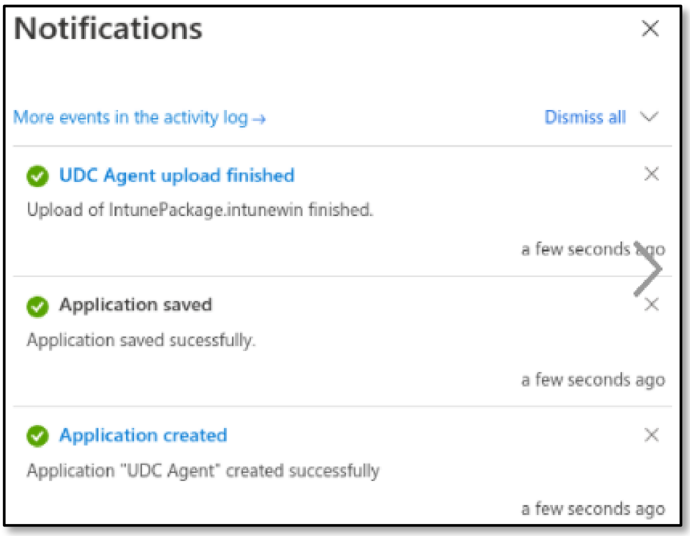
App information

App package file	udc_setup.intunewin
Name	UDC Agent
Description	UDC Agent
Publisher	Lenovo
App Version	3.10
Category	--
Show this as a featured app in the Company Portal	No
Information URL	--
Privacy URL	--
Developer	--
Owner	--
Notes	--
Logo	--

Program

Install command	udc_setup.exe /VERYSILENT /NORESTART
Uninstall command	--
Install behavior	System
Device restart behavior	No specific action
Return codes	0 Success 1707 Success 3010 Soft reboot

Note: When the application is created and uploaded to the system, the following **Notifications** window appears. This process might take an hour or so.



UDC Agent upload finished

Upload of IntunePackage.intunewin finished.

a few seconds ago

Application saved

Application saved sucessfully.

a few seconds ago

Application created

Application "UDC Agent" created successfully

a few seconds ago

Note:

- Now when the LDI agent is installed successfully, you can search for your device in the **Devices** page under the **Device Manager** module.
- Refer to Onboard your fleet for the troubleshooting process.

2.3.8 Deploy Application

You can deploy an application to managed devices, users, or groups.

Note: The deployment process might take between five minutes and an hour to complete.

Following types of deployment are available:

- **Required** – Indicates that the application is required for selected enrolled devices and gets installed automatically. Usually, it happens when you log in to the device.

- **Available for enrolled devices** – Indicates that the application is not required, and you can decide whether to install this application or not. In this case, the application remains in the company portal, and you can install it there.
- **Uninstall** – You can select users or groups for which you want to uninstall the application. The application is uninstalled for the selected managed devices.

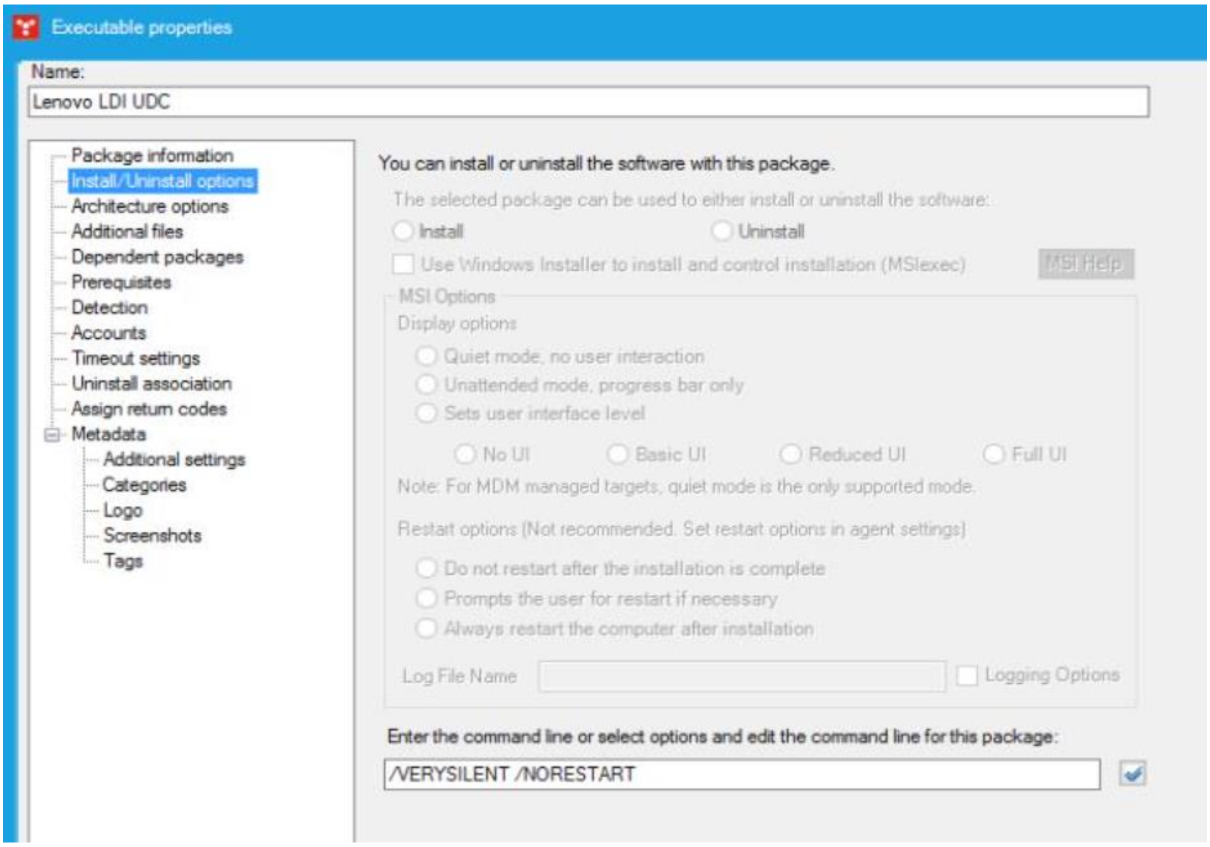
2.4 Ivanti

This chapter allows you to enroll your device in LDI Plus using Ivanti. For this, it provides you an overview of steps to follow to enroll devices.

2.4.1 Executable Properties

Install udc_setup.exe as an executable using the parameters "/VERYSILENT /NORESTART"

Uninstall command:
C:\Windows\System32\drivers\Lenovo\udc\Data\InfBackup\UDCInfInstaller.exe -uninstall



Name: Lenovo LDI UDC

You can install or uninstall the software with this package.

The selected package can be used to either install or uninstall the software:

○ Install ○ Uninstall

□ Use Windows Installer to install and control installation (MSIexec)

MSI Options

Display options

○ Quiet mode, no user interaction

○ Unattended mode, progress bar only

○ Sets user interface level

○ No UI ○ Basic UI ○ Reduced UI ○ Full UI

Note: For MDM managed targets, quiet mode is the only supported mode.

Restart options (Not recommended. Set restart options in agent settings)

○ Do not restart after the installation is complete

○ Prompts the user for restart if necessary

○ Always restart the computer after installation

Log File Name □ Logging Options

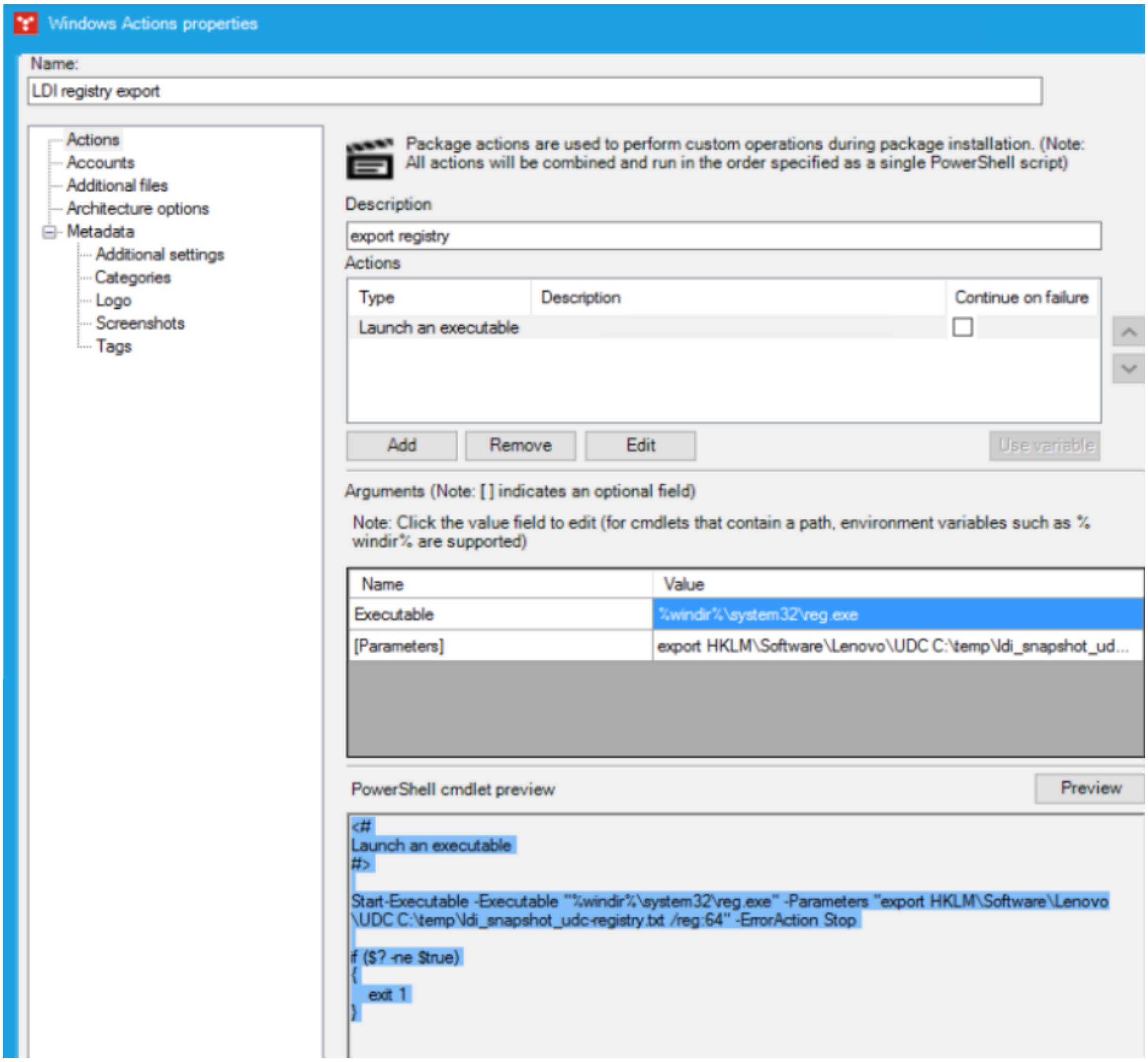
Enter the command line or select options and edit the command line for this package:

/VERYSILENT /NORESTART ☑

2.4.2 Windows Action Properties

Run the registry export as a PowerShell snippet.

Here we assume that the folder c:\temp already exists.



Name:

LDI registry export

Package actions are used to perform custom operations during package installation. (Note: All actions will be combined and run in the order specified as a single PowerShell script)

Description

export registry

Actions

Type	Description	Continue on failure
Launch an executable		□

Arguments (Note: [ ] indicates an optional field)

Note: Click the value field to edit (for cmdlets that contain a path, environment variables such as %windir% are supported)

Name	Value
Executable	%windir%\system32\reg.exe
[Parameters]	export HKLM\Software\Lenovo\UDC C:\temp\ldi_snapshot_ud...

PowerShell cmdlet preview

```
<#
Launch an executable
#>

Start-Executable -Executable "%windir%\system32\reg.exe" -Parameters "export HKLM\Software\Lenovo
\UDC C:\temp\ldi_snapshot_udc-registry.txt /reg:64" -ErrorAction Stop

if ($? -ne $true)
{
  exit 1
}
```

Executable: %windir%\system32\reg.exe

Parameters: export HKLM\Software\Lenovo\UDC C:\temp\ldi\snapshot_udc-registry.txt /reg:64

3 Configure LDI Plus

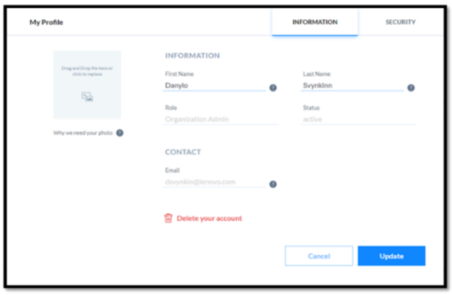
3.1 Manage access

3.1.1 User Creation

Click your user icon in the top ribbon, **My Profile** option.

The following options are available:

- Update your First Name
- Update your Last Name
- Update your Profile Image
- Enable or disable Multi-Factor Authentication.
- Delete your account



My Profile

INFORMATION

First Name: Danylo

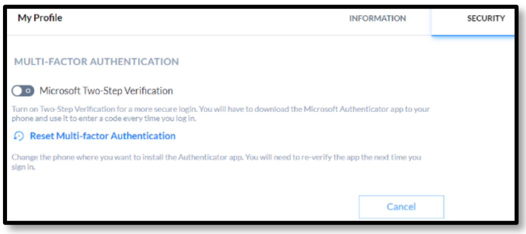
Last Name: Svynkinn

Role: Organization Admin

Status: active

CONTACT

Email: dsvynkin@lenovo.com



My Profile

MULTI-FACTOR AUTHENTICATION

Microsoft Two-Step Verification

Turn on Two-Step Verification for a more secure login. You will have to download the Microsoft Authenticator app to your phone and use it to enter a code every time you log in.

Reset Multi-factor Authentication

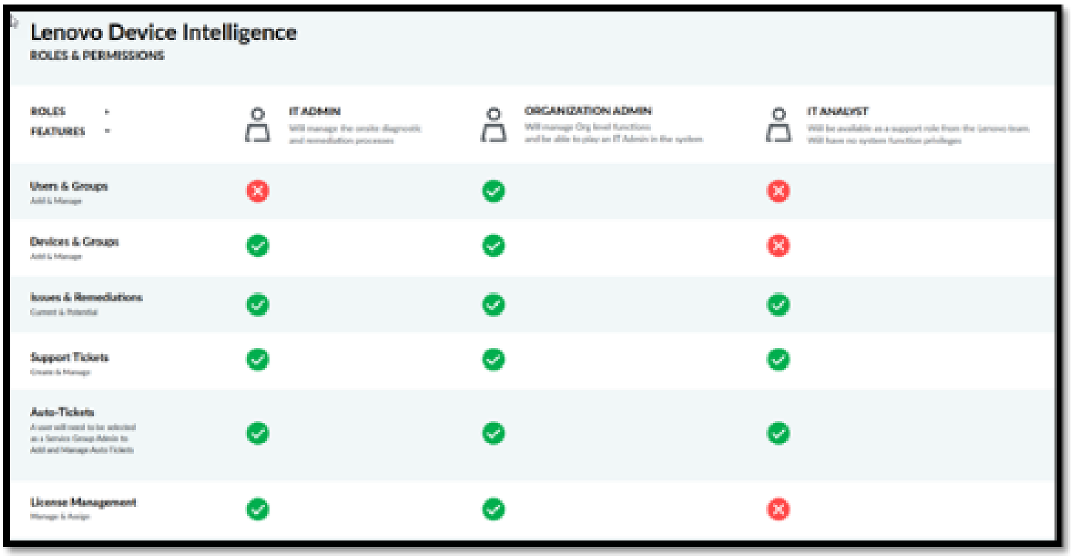
Change the phone where you want to install the Authenticator app. You will need to re-verify the app the next time you sign in.

User Role Types

When you add users to your portal, following role types are available to assign:

- Organization Administrator
- IT Administrator
- IT Analyst

The IT Analyst role can be assigned to a Lenovo Support agent if you would like assistance with an issue.

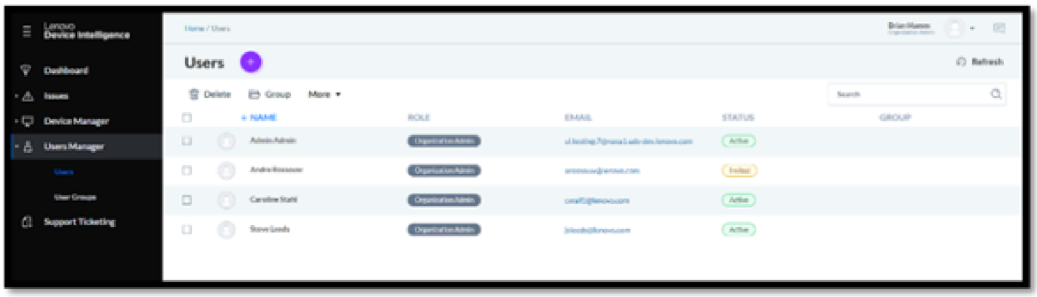


Lenovo Device Intelligence
ROLES & PERMISSIONS

ROLES ▸ FEATURES ▾	IT ADMIN Will manage the onsite diagnostic and remediation processes	ORGANIZATION ADMIN Will manage Org level functions and be able to play an IT Admin in the system	IT ANALYST Will be available as a support role from the Lenovo team. Will have no system function privileges
Users & Groups Add & Manage	✗	✓	✗
Devices & Groups Add & Manage	✓	✓	✗
Issues & Remediations Current & Potential	✓	✓	✓
Support Tickets Create & Manage	✓	✓	✓
Auto-Tickets A user will need to be selected as a Service Group Admin to Add and Manage Auto Tickets	✓	✓	✓
License Management Manage & Assign	✓	✓	✗

View Organization Users

You can manage the users in the portal by selecting **Users Manager → Users**. A table depicts name, role, email, status, and group for each user.



NAME	ROLE	EMAIL	STATUS	GROUP
Admin Admin	Organization Admin	[illegible]	Active	
Andre Rossow	Organization Admin	[illegible]	Invited	
Caroline Stahl	Organization Admin	[illegible]	Active	
Steve Leeds	Organization Admin	[illegible]	Active	

In the **Users** page, you can:

- Invite users
- Delete users
- Group users
- Update users
- Perform bulk updates for users
- Export a list of users to CSV
- View user status
- Invite user(s)

You can add users by accessing **Users Manager → Users → ✚**. You can invite users individually, or in bulk by uploading a CSV file containing user details for each invitee.

To add users individually

1. Click ✚.
2. Enter all the required details.
3. Click **Invite**.

The user receives an email invitation with a link to sign in and/or create a Lenovo ID account using the same email address.

To add users in bulk

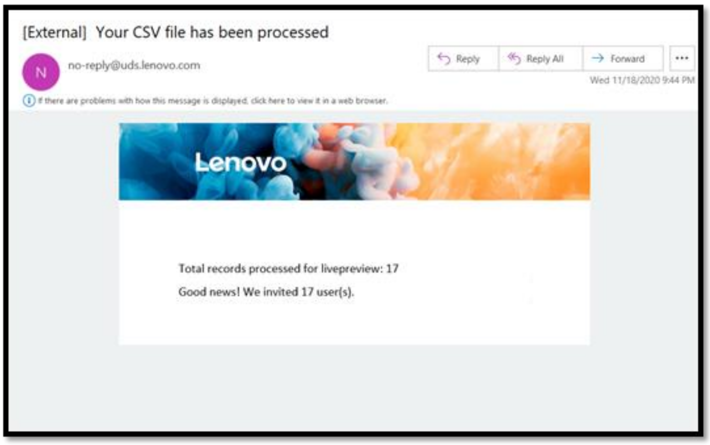
1. Click ✚.
2. Select the **Bulk Invite** tab.
3. Click **Download CSV template** to download CSV template.
4. Populate CSV file with required details for each user - First Name, Last Name, Role, and Email.

For Example: CSV for bulk user invite:

First Name, Last Name, Role, Email
Bill, Lumbergh, Organization Admin,wlumberg@initech.com
Peter, Gibbons, IT Admin, pgibbons@initech.com
Milton, Waddams, Lenovo Device Intelligence Support, mwaddams@initech.com

5. Drop CSV file to the modal window and click **Verify**.

When you upload a CSV file, the file is processed and if there are any errors with the upload, that are displayed in the feedback screen. You receive an e-mail confirmation from the portal when the upload completes.



[External] Your CSV file has been processed

no-reply@uds.lenovo.com

Wed 11/18/2020 9:44 PM

If there are problems with how this message is displayed, click here to view it in a web browser.

Total records processed for livepreview: 17

Good news! We invited 17 user(s).

Note: If a user loses the invitation email, click the user in the Users table to resend the invitation by:

Update User(s)

To manage user information, click a user to open the user tray.

The following options are available for a user on the user tray:

- Update user’s information and contact details (First Name, Last Name, Email, User Role)
- Upload or update a user’s profile image
- Delete a user.

Note: You can also enable multi-factor authentication for a user, if required. By default, it is disabled.

Bulk Updates

Organization or Subscription Admins have the option to Export or Import users in the Users list.

To export user(s) to the .CSV file

1. Select user(s) you want to export (to export all users, make no selection).
2. In the More drop-down list, click **Export**.

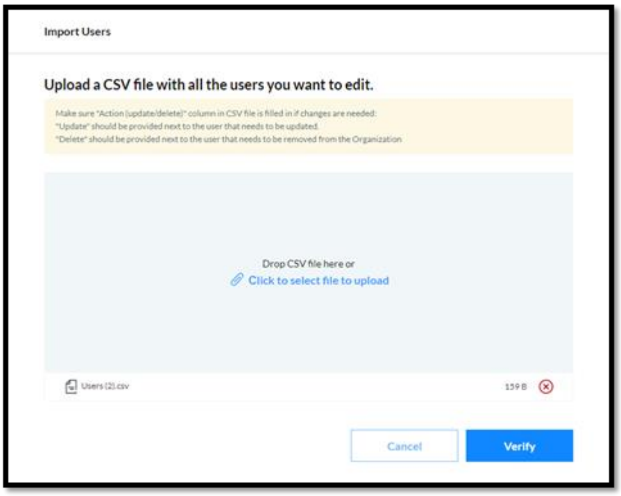
To edit multiple user(s)

Update user fields in the exported users' file.

Note: Make sure **Action** (update/delete) column in the CSV file is filled-in if changes are needed.

- Update should be provided next to the user that needs to be updated.
- Delete should be provided next to the user that needs to be removed from the Organization.

1. In the **More** drop-down list, click **Import**.
2. Drop CSV file to the modal window and click **Verify**.



Import Users

Upload a CSV file with all the users you want to edit.

Make sure "Action (update/delete)" column in CSV file is filled in if changes are needed:
"Update" should be provided next to the user that needs to be updated.
"Delete" should be provided next to the user that needs to be removed from the Organization

Drop CSV file here or
Click to select file to upload

The system validates the uploaded data, and an e-mail confirmation is triggered from the portal when the upload completes.

Use the **Import Results** option to review the results of the import process.

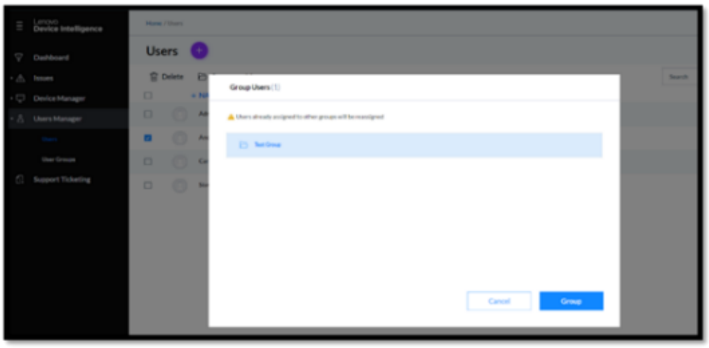
Delete User(s)

1. Select the User(s) you want to delete.
2. Click **Delete** and confirm the deletion.

3.1.2 Assign User(s) to a User Group from the Users page

1. Select the User(s) you want to assign to a user group and click **Group** at the top of the page.

   Note: You can assign a user to an existing group only.



Users already assigned to other groups will be reassigned

2. Select the group you want to assign the user(s) to and click **Assign**.
   Note: Any users already assigned to other groups will be reassigned to the current group as a result of this action.

3.1.2.1. User Groups

Grouping users is helpful for managing a large number, typically by geography, department, or role. User groups can be managed in your portal by accessing **Users Manager** → **User Groups**.

Create user group

3. In the **User Groups** page, click **✚**.
4. Enter the name of the group in **Group Name**.
5. Select users you want to assign to this group.
6. Click **Assign**.

3.1.2.2. Manage User Group

To manage or update group information, click a group to open user group tray.

The following options are available:

- Update group name.
- Add new user(s) to the group.
- Delete user(s) from the group.
- Delete a group.

Delete User Group(s)

1. Select the groups you want to delete.
2. Click **Delete**.

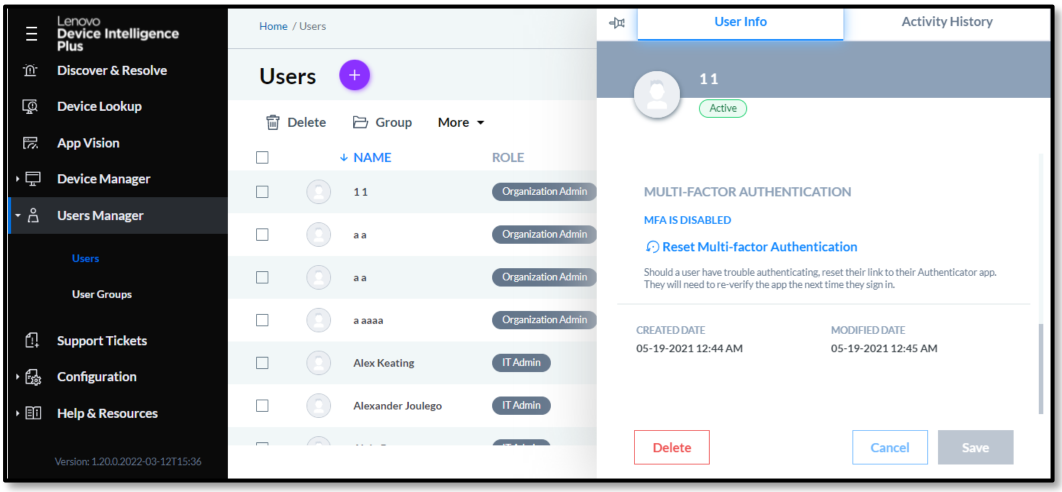
You may also delete a group from the **User Group** tray.

3.1.3 Password change

1. Log in to LDI Plus portal.
2. Click **Forgot Password**. The Reset Password window appears.
3. Enter a new password and click **Next**.
4. Verify your security code. Use the new password to log in to the LDI Plus portal.

3.1.4 Authentication Types

Select **User Manager → Users → User Info** to view the authentication type for users of the solution in your organization.



	NAME	ROLE
□	1 1	Organization Admin
□	a a	Organization Admin
□	a a	Organization Admin
□	a aaaa	Organization Admin
□	Alex Keating	IT Admin
□	Alexander Joulego	IT Admin

MULTI-FACTOR AUTHENTICATION

MFA IS DISABLED

Reset Multi-factor Authentication

Should a user have trouble authenticating, reset their link to their Authenticator app. They will need to re-verify the app the next time they sign in.

CREATED DATE	MODIFIED DATE
05-19-2021 12:44 AM	05-19-2021 12:45 AM

3.1.5 Azure Active Directory, Okta and LenovoID

Azure Active Directory

Azure Active Directory (AAD) registration is supported for several use cases, such as integration with InTune for fleet deployment.

Okta

LDI Plus supports Okta Single Sign On.

Lenovo ID

Lenovo ID is the secure and trusted mechanism providing authentication and identity management for Lenovo Device Intelligence Plus. It offers single sign-on as well as integration with other Lenovo solutions. Lenovo ID accounts can be freely created at passport.lenovo.com. It is not necessary to create the Lenovo ID accounts before users are invited to join by creating an account.

3.2 Manage Devices

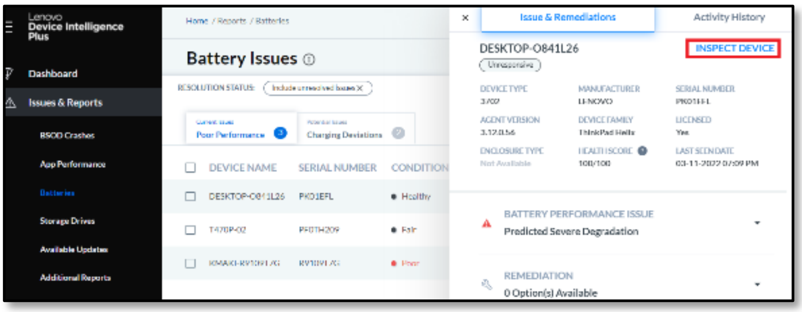
3.2.1 Device manager screens, inspect device fix onboarding issues

For manage devices, refer to Manage Devices.

Inspect Device

You can use Inspect Device to fix the onboarding issues.

1. Click **Inspect Device**.



RESOLUTION STATUS: Include unresolved issues

DEVICE NAME	SERIAL NUMBER	CONDITION
DESKTOP-O841L26	PK01EFL	● Healthy
T470P-02	PF0TH209	● Fair
KMAKI-RV10YLZG	RV10YLZG	● Poor

DESKTOP-O841L26
Unresponsive

DEVICE TYPE	MANUFACTURER	SERIAL NUMBER
3/07	LENOVO	PK01EFL
AGENT VERSION	**DEVICE FAMILY**	**LICENSED**
3.12.0.56	ThinkPad Helix	Yes
ENCLOSURE TYPE	**HEALTH SCORE**	**LAST SEEN DATE**
Not Available	100/100	03-11-2022 07:09 PM

BATTERY PERFORMANCE ISSUE
Predicted Severe Degradation

REMEDIATION
0 Option(s) Available

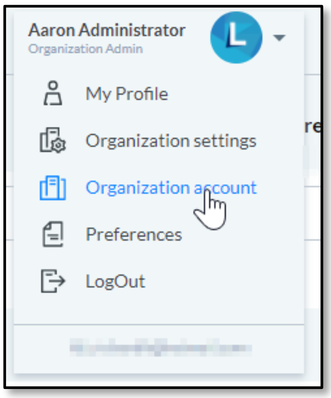
The Device Lookup page appears that shows all the details of the device, issues, sensors, health analysis, installed application, and hardware component related issues. Based on the details, you can fix the issues.

3.3 Org Settings vs Configuration

3.3.1 Organization Setup

When your organization's portal is created, a single administrative account is also created. The IT Owner specified to Lenovo at the time of sale receives a Lenovo Device Intelligence Plus e-mail regarding access to your organization. When you click the link, you are taken to the **Sign on** page log in to LDI Plus as an Organization Administrator.

With this administrative account, you can configure the portal, invite users, and add devices.



3.3.2 Manage Organization

Important Note: Some of the following settings may not appear if your organization is in a Trial program.

Profile

Manage the profile for your organization, including logo, organization name, country, and address.

Licenses

View the licenses assigned to your organization, their quantities, and usage. A link is available to manage license assignment on a per-device basis.

When a device is unlicensed due to assignment or expiration, you can expect the following:

- Data from the device is not collected or processed
- Previous data for the device is preserved
- The device is excluded from reports and intelligence

Authentication

View the authentication type for users of the solution in your organization. You can view the settings for your organization when you click on the user icon in the top ribbon Organization Account option.

The following options are available:

- Update Organization Name
- Update Organization Country
- Update Organization Website
- Update Organization Address
- Update Organization Profile Image

User Preferences

You can access the preferences for your user account when you click on the user Icon in the top ribbon Preferences option.

Preferences page allows you to manage portal language, email frequency, and view Terms & Conditions with Privacy Policy.

Language

The language that the portal UI is displayed in.

3.3.2.1. Set Portal Languange

You can configure the portal language in the Portal Preferences page.

1. In the LDI Plus portal, click the User drop-down list.
2. Select Preferences.
3. In the **Settings** section, select a desired language in the **Language** drop-down list.
4. Click **OK**.

Note: Wait for approximately 30 minutes to reflect the change.

You can configure the following languages:

- Deutsch (DE)
- English (EN)
- Español (ES)
- Français (FR)
- 日本語 (JA)
- Português (PT)

- 中文 (ZH)

Email Frequency

Daily Email Summary: Start your day with an update of a daily snapshot of all the current and potential issues in your fleet.

3.4 Organization Settings

Before you use LDI APIs, you must generate API credentials in the LDI account.

1. Click **Organization Settings** in the **Organization Admin** window.
2. Click **API Credentials** in the **Organization Settings** window. The **API Credentials** pane appears. If there are no API credentials, click **Generate** to create the credentials.

Note: A Client ID and Secret key are generated. You can copy them to the clipboard. If you want to change the existing API credentials, you can generate a new one.

3. Click **Regenerate**. The **Regenerate** pop-up window appears.
4. Click **Regenerate**. A new Client ID and Secret key is generated.

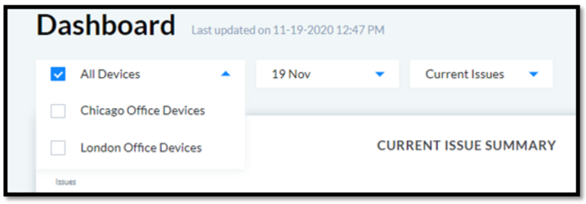
4 Monitor your fleet

4.1 Dashboards

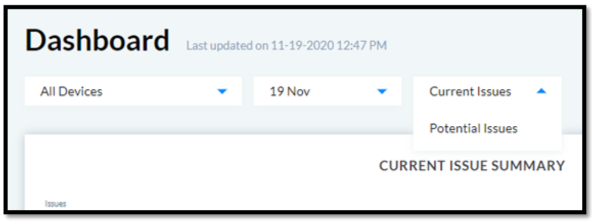
Dashboard is the home page for Lenovo Device Intelligence Plus and offers an overview of the devices in your organization. The Dashboard consists of several cards, where each card represents one or many insight categories. Issues are how items are tracked for each insightcategory; clicking on metrics displayed on a chart or below a particular widget navigates theuser to the corresponding Issue Report Page, which provides a device-by-device list of issues. All widgets are of the same size to allow continuity with the dashboard.

Note: Issue data is displayed for the last 24 hours by default. Facets are available at the top of the dashboard to filter by:

Device Groups



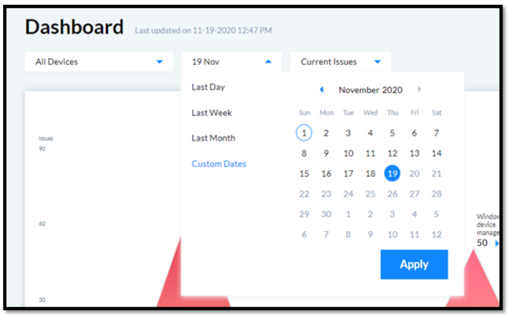
Detected and predicted issues



Date range filter

Selecting a date range filter causes the Dashboard to refresh with the data associated withthe selected date range.

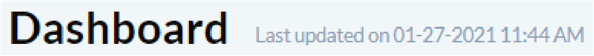
Note: The following Dashboard widgets are not affected by the Date Filter: Health Score, Device Counts, and Licensing (if available).



Filtering by date provides a historical view of your devices fleet in each insight category that allows you to view and analyses how the state of your devices has changed over time.

Filtering by a date range causes some Dashboard charts to transform into a trend line todisplay issues over time.

Date/Time Refresh now corresponds to when the data was last refreshed in the organization.



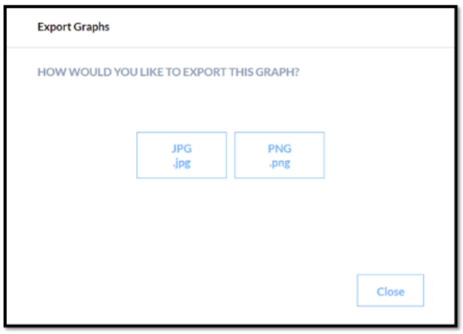
Dashboard Last updated on 01-27-2021 11:44 AM

4.1.1 Dashboard Enhancements

Expanded Dashboard Widgets

Dashboard widgets can be exported.

1. Click the ellipsis found on the upper right-hand corner of the widget.
2. Select Export Graphs.



Export Graphs

HOW WOULD YOU LIKE TO EXPORT THIS GRAPH?

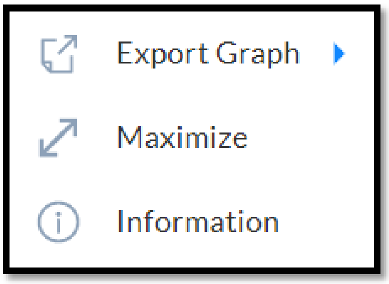
You can select JPG or PNG file types.

Maximize Widgets

Dashboard widgets that contain information may be expanded.

1. Click on the ellipsis found on the upper right-hand corner of the widget.
2. Choose **Maximize**.

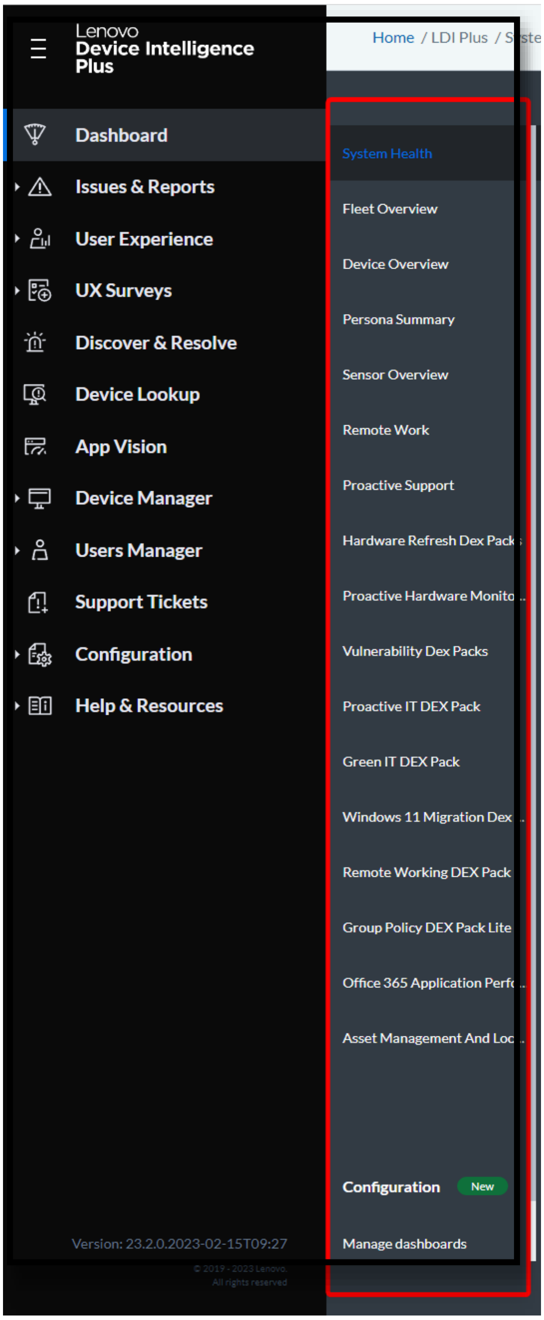
Note: If there is no data in a widget, the Maximize option is not available for that widget.



3. Click **Close** to return to the dashboard.

4.1.1.1. Dashboard Side-menu

A new side menu is added to the dashboard tab in LDI Plus. The menu has System Health, Fleet Overview, Device Overview, Persona Summary, Sensor Overview, RemoteWork, and Proactive Support which give a comprehensive dashboard view of the vital metrics at the device and fleet level.



System Health

Measures the functionality of your environment and its ability to support your users. The following table describes the Dashboard widgets:

Widget Name	Description
Support Tickets	Number of tickets submitted in the portal, if applicable, with quick links to see the details and status.

Device Status	Number of devices onboarded to LDI Plus, categorized by status.
Device Licenses	Number of unassigned licenses vs. the number of assigned licenses
Current Issue Summary	Visualizes the summary of issues by type - Current or Potential
Overall Health Score	A calculated score based on the mix of current, monitored, and predicted issues and can be used for ahigh-level assessment of the health of your fleet.
Blue Screen of Death Crashes (BSOD)	For current data, this shows BSODs that were detected for the selected time range. For potential, this showshow many BSODs are predicted to happen at a point.
Applications Impacting Performance	For current and potential issues, this widget calls out any applications that have caused a performance impact on the CPU, or that are predicted to do so based on deep learning AI modelling.
Batteries	Displays the devices with the performance, charging, or discharging battery issues.
Storage Drives	Displays the devices that have HDDs or SSDs relatedissues.
Available Updates	Displays the updates available for the fleet grouped by top affected device manufacturer and model.

Fleet Overview

Provides CIOs with a real-time view of what is happening within key organizational groups acrossthe entire computing landscape.

Device Overview

Provides an IT manager perspective of specific systems and users with more in-depthproblem diagnostics.

Persona Analysis

Provides abstract models of real users based on work patterns, behavior, and tools of actualusers in the environment. Personas allow IT to distil users1 down to a manageable number of user types and understand what a persona requires from a hardware, software, mobility,security, and software perspective. Knowing these requirements aids in effectively provisioning support resources, including budget and personnel, to maximize the end user experience.

Sensor Overview

Shows how common a problem might be across a fleet of devices and can be hidden ifdesired to hide an alert that is not relevant to your organization.

Remote Work

The pane in the Remote Work tab is divided into different cards.

DEM (Digital Experience Monitoring) - User Experience Trend – A representation in the form of bar graph that indicates the user experience of using a device or group of devices based on the data gathered from the device or fleet of devices for a specific time. As you discover issues and fix them, the trend changes over the time.

Top 5 Health Impacts – A pie-chart representation of top 5 impacts to the end-userexperience. A bigger slice of pie chart indicates that greater attention must be paidto that metric as it is negatively impacting user experience more than others.

Digital Experience Tools – A pie-chart presentation of the important metrics or parametersthat impact remote work/collaboration, like office connectivity, security and compliance, productivity and collaboration and device. The metrics that have larger share of the pie- chart are impacting more, because more problems are occurring there.

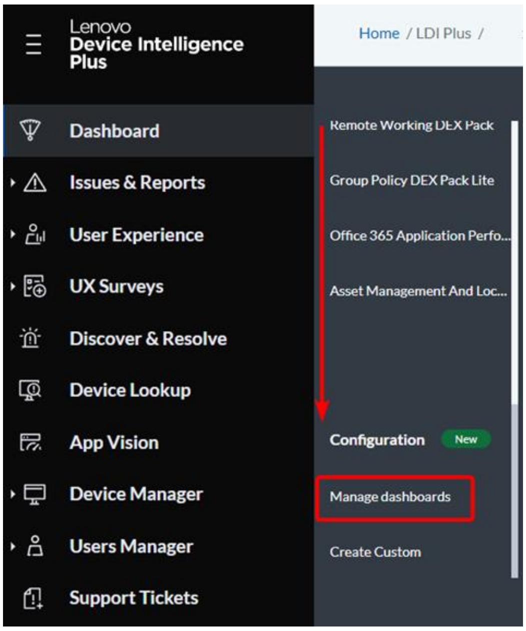
Machine Sizing – A pie-chart presentation machine sizing for the system or group of devicesin context to the hardware utilized. Whether it is over provisioned, under provisioned or is right-sized.

Proactive Support - The pane in the proactive tab is divided into different cards that help you in supporting your users proactively.

4.1.1.2. Configuration

4.1.1.2.1. Manage Dashboard

A new side menu is added to the dashboard tab in LDI Plus. This gives a configurable overview of which dashboards are enabled and in what order for your organization.



Below is a list of the available DEX packs that your organization can enable for additional analysis.

Critical App Details

View the critical app details and current versions that are installed on the systems.

Machine Right Sizing

Shows the resource consumption of a device and makes a recommendation on re-sizing based on user needs.

What Is the End User Experience of My Estate

Answers the question of what groups of users have a worsening experience and what the issues are.

Windows Patch Details

The dashboard provides a breakdown of patched and unpatched systems, patch details, and install details for Windows KB.

Application Latency Service Map

This dashboard provides a group-based summary of application dependencies organized by domain and subnet to help trace potential issues with routing or latency.

Application Network Performance Overview

This dashboard summarizes application network consumption and performance for a selected group of devices. This can help illustrate potential sources of high bandwidth usage that may be problematic in scenarios with limited connectivity.

Asset Management and Location Summary

This dashboard summarizes the location of devices (using egress IP detection) with some asset details. This can help keep track of the physical location of distributed devices.

Collaboration Tool Details

The dashboard summarizes app average resource consumption and app usage over a selected period of time.

Digital Experience Unboxed by Group

The dashboard summarizes Digital Experience of the fleet that can be viewed by groups. The system provides information about categories, that impact Digital Experience, the issue, and sensor trends within the last few days.

End User Experience Trend by Group

This dashboard provides visibility into the health trend over the past thirty days with a focus on providing an analysis of the key impact sources over the course of the last month. Selection of an individual day will provide a review of the user experience impacts for systems on that selected day.

Executive Group Comparison

This dashboard provides a quick, group-based summary of user experience and performance for devices.

Office 365 Application Performance Overview

This dashboard provides an overview of Office suite application usage and performance characteristics for the enterprise. Note that this dashboard does not require connection to the Office 365 API.

Remote Worker Performance Impact

Compare performance across multiple systems before and during remote work.

Target Application Network Performance

This dashboard identifies application network consumption and performance for a selected application for a group of devices. This can help illustrate potential sources of high bandwidth usage that may be problematic in scenarios with limited connectivity.

Workforce Connectivity Habits

This dashboard summarizes the security characteristics of connections made by a selected group of devices.

Hardware Refresh Dex Packs

This DEX Pack analyses health, age, CPU storage, C: Drive Storage, Memory, and other metrics to determine necessity of upgrading or replacing hardware. External monitor recommendations are also included in this pack.

Proactive Hardware Monitoring Dex Packs

Monitors hardware performance, issues, and inventory.

Windows 11 Migration Dex Packs

This DEX Pack is designed to assist with your journey to Windows 11. Determine hardware and application readiness, identify actions to take to get your estate ready, assess Windows 11 performance and monitor the progress of the rollout.

Vulnerability Dex Packs

This DEX Pack provides actionable data in order to determine the impacts, spread, and relative vulnerability throughout your enterprise.

Remote Working Dex Pack

This DEX Pack helps you understand the needs, work habits, and user experience of your remote workforce. Discover how remote workers connect to the corporate network, and assess how this connection impacts productivity, user experience, and security risk.

Proactive IT Dex Pack

A proactive IT support strategy can address many of the deficiencies of the reactive, break/fix model. Use this DEX Pack to gain greater visibility and insight into potential problems and act before problems cause significant downtime.

Green IT Dex Pack

This DEX Pack facilitates green computing by monitoring energy consumption. Use these dashboards to determine which groups, regions, and models have the highest environmental impact. This data covers a variety of systems, including printers and virtual machines. This DEX Pack guides decisions to reduce energy and printing costs.

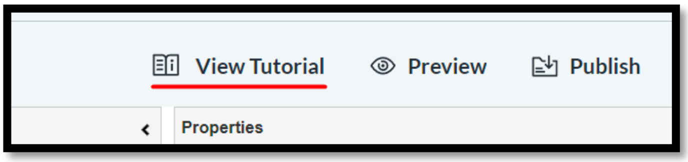
Group Policy Dex Pack Lite

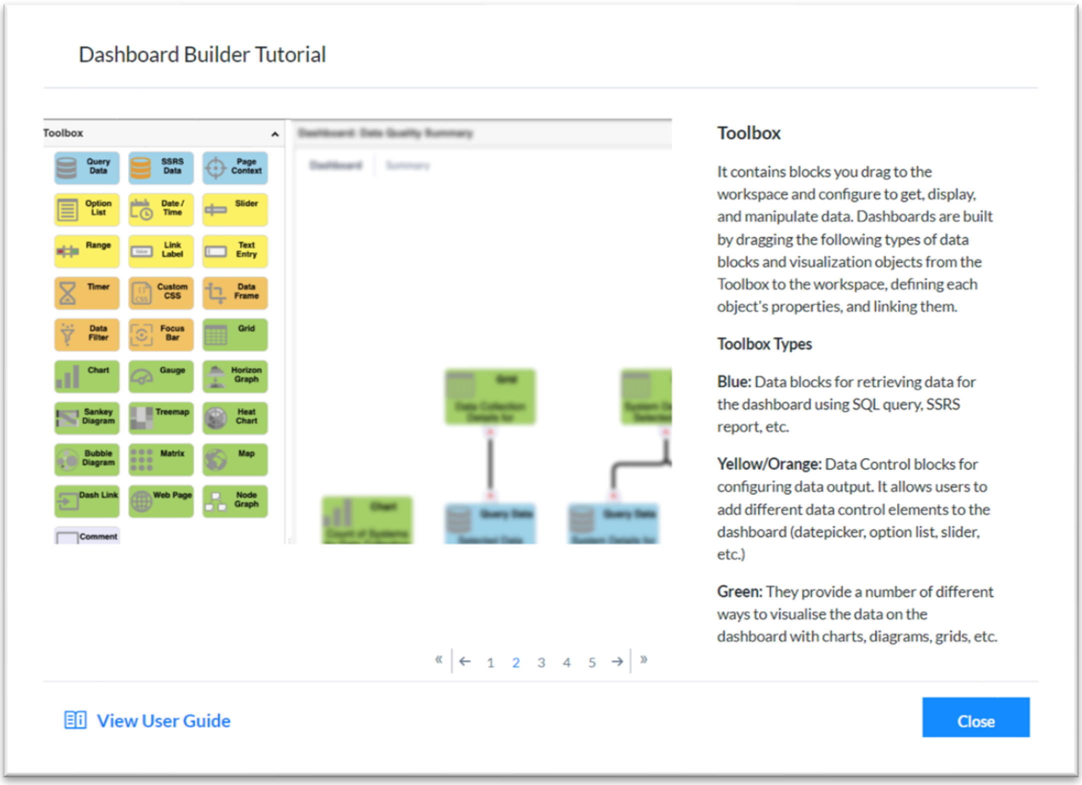
Shows group policy usage and compliance.

4.1.1.3. Dashboard Builder

The new Dashboard Builder feature gives LDI Plus a new way to interact with the data that has been collected across the fleet of devices. While most of the data is viewable across the many different dashboards already provided, Dashboard Builder allows LDI Plus users to create entirely custom views for instances where there is a need for viewing specific data such as the Windows 11 Migration dashboard used to compare devices in the fleet to Microsoft's minimum Windows 11 system requirements.

When you open Manage Dashboards page and use the + icon to Create a New Dashboard there is a "View Tutorial" option available for you to get a brief introduction to the many tools on the page.




Dashboard Builder Tutorial

Toolbox

It contains blocks you drag to the workspace and configure to get, display, and manipulate data. Dashboards are built by dragging the following types of data blocks and visualization objects from the Toolbox to the workspace, defining each object's properties, and linking them.

Toolbox Types

Blue: Data blocks for retrieving data for the dashboard using SQL query, SSRS report, etc.

Yellow/Orange: Data Control blocks for configuring data output. It allows users to add different data control elements to the dashboard (datepicker, option list, slider, etc.)

Green: They provide a number of different ways to visualise the data on the dashboard with charts, diagrams, grids, etc.

There is additional Dashboard Builder documentation available on the LDI Plus Support Site to guide you more thoroughly through the different aspects of the toolset.

4.2 Issues and Reports

Reports help you identify and act on issues that may result from BSOD crashes, app performance, batteries, storage drives, and device errors. By categorizing these problems inan easy-to-read layout, this module provides a way to view current and potential future issues briefly, giving the IT personnel an opportunity to be proactive instead of reactive.

4.2.1 System Crashes (BSODs)

System crashes for Windows devices are commonly referred to as **Blue Screen of Death**. LDIPlus uses artificial intelligence to analyse device hardware, drivers, and OS events to highlight crashes that are currently occurring or likely to occur in the future.

Detected Crashes

This report provides details about crashes that have recently occurred on devices withinyour organization.

Frequently Crashing

This report can identify trending crashes on devise within your organization. This can helpyou tackle the most troublesome crashes that may be impacting the device experience.

Predicted Crashes

This report uses AI to identify crash trends and predict which devices are likely to encountersimilar crashes. Responding to predictions in this report enables you to fix problems before they occur.

Date filtering provides a historical view of the issues that affected devices fleet before. Youcan filter BSOD Issues by various columns.

When you click a device, the system displays the Issue Tray, which provides details aboutthe findings and remediations.

Application Performance Insights

A process can be a driver, UI application, or background service, and an average PC may have 100 - 200 processes running at a time. Each process consumes from a limited resourcepool of memory, disk I/O, network, and most importantly, CPU. LDI Plus uses on-device AI to identify processes that are exhibiting abnormal resource usage that may be impacting theperformance of the whole PC and may be an early indicator for further issues that could be observed in your fleet.

Batteries

Batteries enables you to work while on a plane, in a meeting, or on the couch. A computer user with a poor performing battery experiences a diminished work experience, and may be limited regarding how, where, and when they work. All batteries naturally degrade over time,but some batteries may degrade faster than others due to user behaviour, environment conditions, or manufacturer quality defects.

Replacement and repair of devices or parts of devices is available pursuant to the terms of an applicable Lenovo warranty.

Poor Performance

This report can identify devices with batteries that are under performing into their expected charge. Devices marked as poor condition are unable to remain unplugged for long.

Charging Deviations

AI-based anomaly detection that detects devices who are experiencing charging behaviour that is irregular when compared to normal charging trends. A change in the charging characteristics may be indicative of a new or recent change on the device that could induceirregular power consumption.

Storage Drives

Storage reports aggregate data from storage drives such as Hard Disk Drive (HDD), Solid State Drive (SSD), and Non-Volatile Memory Express (NVME) within your organization andhighlight concerning issues using factors such as drive capacity, S.M.A.R.T monitoring, temperature, and firmware. A problematic storage device may result in frequent crashing, loss of time, or permanent loss of work.

All Detected

You can use this report to identify devices with storage drives that are currently problematic. This report also helps you to identify user devices that may need a drivereplacement or clean-up.

High Risk

This report uses AI to identify storage failure trends and **predict** which devices may soon have a high-risk issue. Responding to predictions in this report enables you to fix problemsbefore they occur.

Medium Risk

This report uses AI to identify storage failure trends and **predict** which devices may soonhave a medium-risk issue. Responding to predictions in this report enables you to fix problems before they occur.

Out of Capacity

This report displays the devices that run out of capacity in next 30 days.

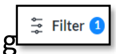
Available Updates

This report displays the devices that have BIOS and Thunderbolt-related updates available inthe tool.

Additional Reports

This feature allows you to analyse reports and select their different download format.

Report Filtering



Report filtering functionality allows you to filter the list of issues by filter criteria(defined columns by which the list can be filtered - unique for each issue report and its tab) displayed in the **Filter Data** modal window.

You can use following types of filtering:

Multi-Select filtering: Available for qualitative filter criteria to group by unique items represented in the issue list. Filter criteria list contains the list of unique filter criteria itemsthat are presented in the history of the defined issues list.

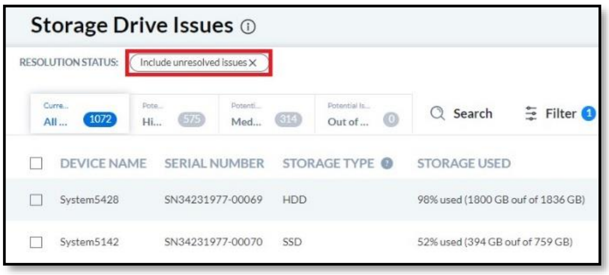
Range filtering: Available for numeric filter criteria to filter by a specific range of numericvalues. Filter criteria range slider allows selecting the range within the min and maximumfilter criteria numeric values that are presented in the history of the defined issues list.

Exporting Reports to CSV

To perform Issues List export, click the Export List icon to export the selected BSOD crashes report in the .csv file format. If there were filters applied, then confirm if you wantto export with or without filters applied.

Note: You must apply filters before exporting report/reports. Otherwise, you get the details of all the devices' issues.

To remove the filter, click ✕ .



Storage Drive Issues ⓘ

RESOLUTION STATUS: Include unresolved issues ✕

Curre... All ... 1072 | Pote... Hi... 575 | Potenti... Med... 314 | Potential Is... Out of ... 0 | Search | Filter 1

□	DEVICE NAME	SERIAL NUMBER	STORAGE TYPE	STORAGE USED
□	System5428	SN34231977-00069	HDD	98% used (1800 GB ouf of 1836 GB)
□	System5142	SN34231977-00070	SSD	52% used (394 GB ouf of 759 GB)

Issue Tray

When you click a particular device row in an Issue Report, the Issue Tray window isdisplayed as a slide-in from the right side of the window.

The Issue Tray contains two tabs:

- **Issue & Remediations** - Information about the device that experienced the selected issue, the issue details, and the remediations.
- **Activity History** - Feedback for a remediation or issue itself to improve the remediations that are shown for issues.

Click Raise a Lenovo Support Ticket to raise a support ticket.

Other Features

Searching Functionality

Click Search to find a device or issue in a list or report table. Search supports single andmultiple character wildcard searches using ? and *.

- The single character wildcard search **(?)** looks for terms that match that

with the single character replaced. For example, to search for **text** or **test**,

you can input **te?t**.

- Multiple character wildcard search **(*)** looks for 0 or more characters. For

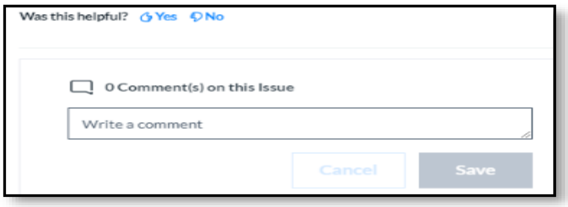
example, to search for Windows, Windows95, or WindowsNT, enter **win***.

Issues Feedback

This data is gathered and used to prioritize the remediations shown for a given issue in thefuture.

To send feedback positive or negative for a particular issue, click **Yes** or **No** in the issue tray. The system displays the feedback modal window with the list of options for selection. Enter details to the displayed text area if any, then click **Send**.

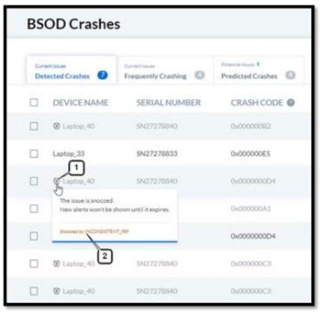
To provide a comment regarding your experience with the tool, enter text in the box comment text and click **Save**.



Snooze

The Snooze feature allows you to snooze not-so-important issues so that you can focus onmore important ones that need attention/remediation on a priority basis. You can use this feature to:

- Snooze a specific issue on one or more device, or all devices in the organization
- Create a rule, which is a set of issues or a single issue and apply it on specific devicesor entire fleet of devices.
- Select the duration for which the device(s) can be snoozed. It can be for a day, week, month, or year.
- Snooze feature is available for Organization Admin, IT Admin, and IT Analyst accounts.



☐	DEVICE NAME	SERIAL NUMBER	CRASH CODE
☐	Laptop_40	SN27278840	0x000000B2
☐	Laptop_33	SN27278833	0x000000E5
☐	Laptop_40	SN27278840	0x000000D4
☐			0x000000A1
☐			0x000000D4
☐	Laptop_40	SN27278840	0x000000C3
☐	Laptop_40	SN27278840	0x000000C3

The issue is snoozed.
New alerts won't be shown until it expires.

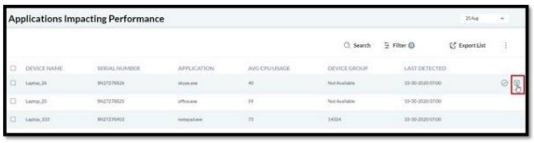
Snoozed by INCONSISTENT_IRP

The snooze icon shows that the device has been snoozed for a specific issue. Name or type of issue for which the device has been snoozed. A device can be snoozed for multiple issues.

You can use the snooze feature is different ways. They are:

Snooze an Issue on a Single Device

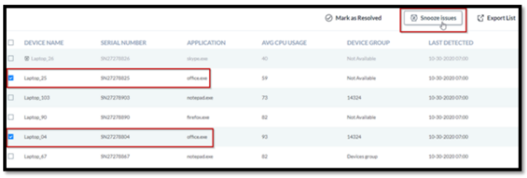
1. Click **Snooze** icon in the device row. You see a modal window.



☐	DEVICE NAME	SERIAL NUMBER	APPLICATION	AVG CPU USAGE	DEVICE GROUP	LAST DETECTED
☐	Laptop_26	SN27278826	skype.exe	40	Not Available	10-30-2020 07:00
☐	Laptop_25	SN27278825	office.exe	59	Not Available	10-30-2020 07:00
☐	Laptop_103	SN27278903	notepad.exe	73	14324	10-30-2020 07:00

2. Select the duration from the available options.
3. Click **Snooze**. The device is snoozed. You can see that snooze icon appears before thedevice name.

Snooze Same Issue(s) on Multiple Devices

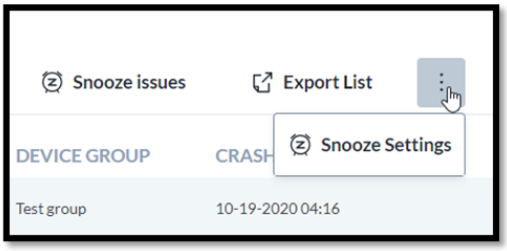


☐	DEVICE NAME	SERIAL NUMBER	APPLICATION	AVG CPU USAGE	DEVICE GROUP	LAST DETECTED
☐	Laptop_26	SN27278826	skype.exe	40	Not Available	10-30-2020 07:00
☑	Laptop_25	SN27278825	office.exe	59	Not Available	10-30-2020 07:00
☐	Laptop_103	SN27278903	notepad.exe	73	14324	10-30-2020 07:00
☐	Laptop_90	SN27278890	firefox.exe	82	Not Available	10-30-2020 07:00
☑	Laptop_04	SN27278804	office.exe	93	14324	10-30-2020 07:00
☐	Laptop_67	SN27278867	notepad.exe	82	Devices group	10-30-2020 07:00

1. Select the checkboxes against the device names with same issue(s).
2. Click **Snooze Issues**. You see a modal window.
3. Select the duration to snooze the devices.

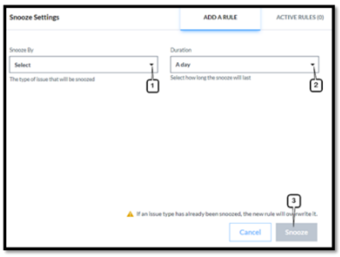
> If you mark the checkbox then all devices in the organization will be snoozed for the specific issue(s).

4. Mark the checkbox- Apply to any device with the same issue(s).
5. Click **Snooze**. Both devices with same issue are snoozed.
6. Create a Snooze Rule and Implement on Selected Device(s)



Test group 10-19-2020 04:16

7. Click **Ellipsis**. You see the **Snooze Settings** button.
8. Click **Snooze Setting**. The **Snooze Settings** pop-up window appears.



Snooze By: Select

The type of issue that will be snoozed

Duration: A day

Select how long the snooze will last

⚠ If an issue type has already been snoozed, the new rule will overwrite it.

ADD A RULE is the default tab and on the default pane you can:

9. Select the issue to snooze in the **Snooze By** drop-down list.
10. Select the duration for which device is to be snoozed.
11. Click **Snooze**.

You can select multiple issues from the **Snooze By** drop-down list for specific duration.

You can create new rules by using the ADD A RULE tab. All the rules created can be viewedin the ACTIVE RULES tab.

12. Click Ellipsis.
13. Click Snooze Settings. The Snooze Settings window appears.
14. Select the issues from the drop-down list in **Snooze By** field. The device(s) is snoozed for selected issues.
15. Select duration. It is the time for which the device is snoozed for the selected issue(s).

16. Click **Snooze**. All devices are snoozed for the selected issues.

Unsnooze the Snoozed Issues

You can unsnooze the snoozed devices in three different ways:

1. Click ⊗ from the device row. You see a modal window.
2. Select the Only for this Device option.

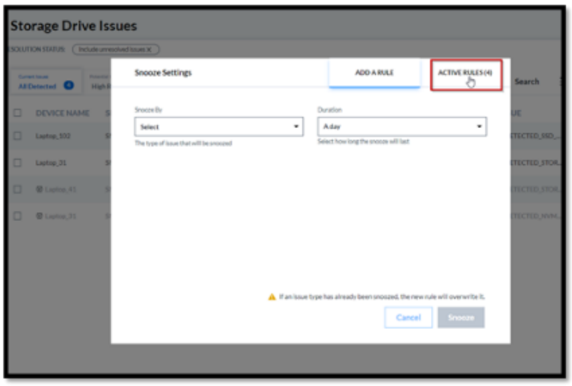
> If you select the radio button – For any device - then all devices which were snoozed for specific issue(s), will be unsnoozed.

3. Click **Unsnooze**. The device is unsnoozed.

Unsnooze from the Device Tray

1. Click the device row. The device tray window appears.
2. Click the downward arrow in the **Actions** tab. A menu pops up.
3. Click **Unsnooze** issue. You see a modal window.
4. Select the Only for this device option.
5. Click **Unsnooze**. The issue is unsnoozed on the device.

Unsnooze from the Active Rules tab



Snooze By: Select
The type of issue that will be snoozed

Duration: A day
Select how long the snooze will last

⚠ If an issue type has already been snoozed, the new rule will overwrite it.

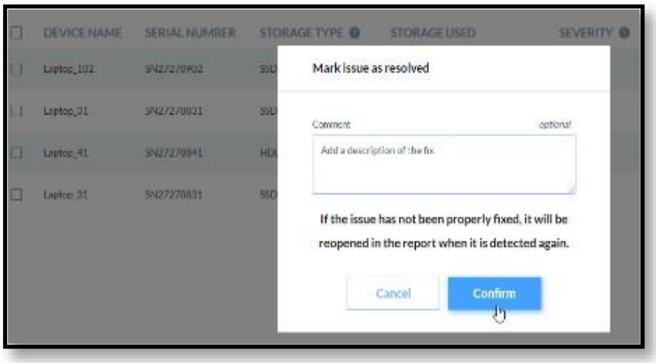
6. Click **Active Rules** tab. The **Snooze Settings** window appears.
7. Select the **Snoozed Issue** type checkbox in header of the table. All issue types aremarked.
8. Click **Unsnooze**. All the issue types on all devices are unsnoozed.

> In the Active Rules Tab, following are the headers:
>
> 1. **Snoozed Issue Type** – Lists different types of issues that are snoozed
>
> 2. **Applied To** - Mentions the serial number of the device(s) on whom issue(s) have been snoozed. When *"Any Device"* is mentioned then it means that all devices in the organization or fleet having the same issue type(s) will be snoozed for that issue(s).
>
> 3. **Except** - Mentions the serial number(s) of the device(s) on which snooze rule is not applied.
>
> 4. **Expires At** – Indicates the time and date of expiry of the snooze rule.

Note:

You can now mark an issue on a device as resolved. A green-colored Right icon ✓ appears before the name of the device. If you hover the cursor on the icon amessage box pops up. The row is greyed out.

4.2.1. Mark the Issue as Resolved



DEVICE NAME	SERIAL NUMBER	STORAGE TYPE	STORAGE USED	SEVERITY
Laptop_102	SN27278902	SSD		
Laptop_31	SN27278831	SSD		
Laptop_41	SN27278841	HD		
Laptop_31	SN27278831	SSD		

Mark Issue as resolved

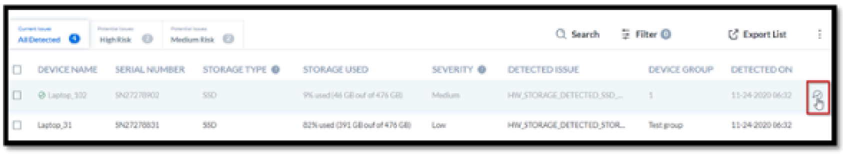
Comment optional

Add a description of the fix

If the issue has not been properly fixed, it will be reopened in the report when it is detected again.

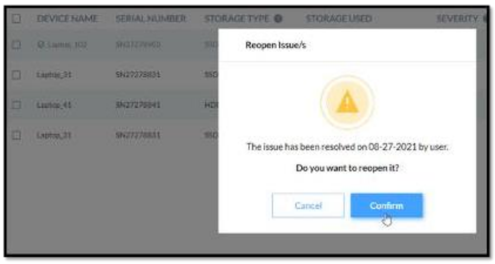
1. Click on Right Icon. You see a modal window.
2. Enter comment in the comment box (optional).
3. Click **Confirm**.

Reopen the Resolved issue



□	DEVICE NAME	SERIAL NUMBER	STORAGE TYPE	STORAGE USED	SEVERITY	DETECTED ISSUE	DEVICE GROUP	DETECTED ON
□	Laptop_102	SN27278902	SSD	9% used (46 GB out of 476 GB)	Medium	HW_STORAGE_DETECTED_SSD_...	1	11-24-2020 06:32
□	Laptop_31	SN27278831	SSD	82% used (391 GB out of 476 GB)	Low	HW_STORAGE_DETECTED_STOR...	Test group	11-24-2020 06:32

4. Click on the Right Icon. A window appears.



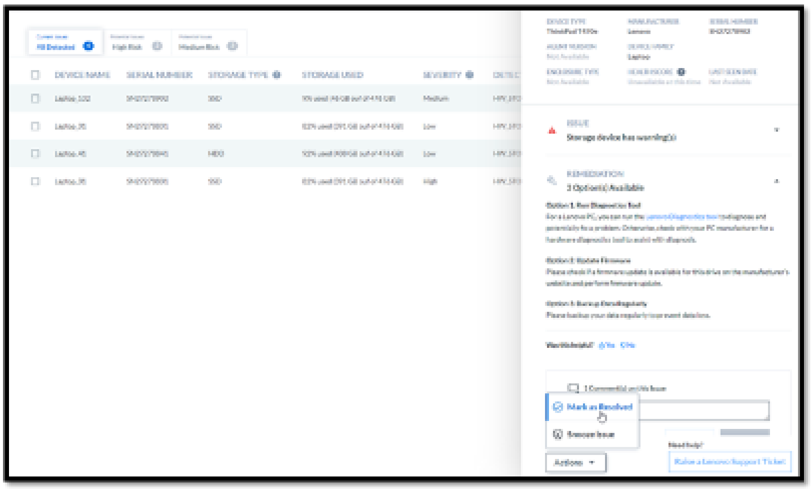
Reopen Issue/s

The issue has been resolved on 08-27-2021 by user.

Do you want to reopen it?

5. Click **Confirm** to reopen the issue.

You can also resolve and reopen the resolved issue from the device tray.



4.3 Discover and Resolve

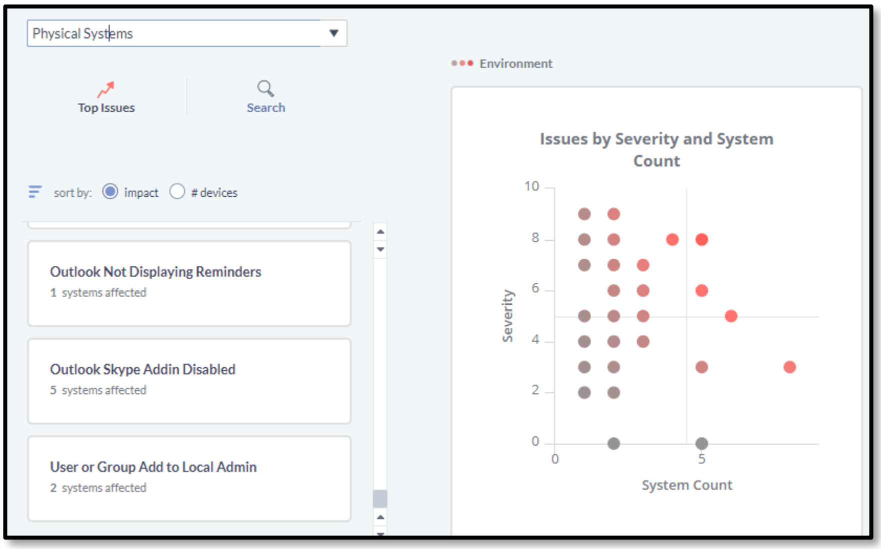
The AI component of Discover & Resolve correlates and analyses many components at the same time. Discover & Resolve combines root cause analysis and self-healing functions intoone tool and compares trends and patterns to create predictive insights for those remediation efforts.

Key Benefits

- Detects and predicts anomalies and patterns
- Resolves issues before user impact
- Creates a more effective support process
- Results in enhanced user productivity

Daily Issues

Provides you details of issues occurring for the system selected in the **Systems** drop-down list on the current day.



Physical Systems

sort by: ● impact ○ # devices

Outlook Not Displaying Reminders
1 systems affected

Outlook Skype Addin Disabled
5 systems affected

User or Group Add to Local Admin
2 systems affected

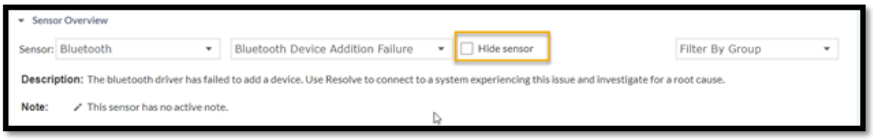
Sensors

LDI Plus uses Sensors to provide context-based alerts about situations that may require attention. By providing real-time investigations into the environment, Sensors help pointyou in the right direction to troubleshoot a system or group of systems and avoid IT blindspots.

Sensors help show how common a problem might be across a fleet of devices and can be

hidden if desired to hide an alert that isn’t relevant to your organization. LDI Plus features avariety of sensors in categories such as Management, Memory, Microsoft Office, Security, System, and more.

To hide a Sensor, select **Discover & Resolve** and then **Sensor Details**. You can choose a Sensor in the drop-down list and select the box beside Hide Sensor to remove itfrom your viewable Sensor list.



Sensor Overview

Sensor: Bluetooth

Bluetooth Device Addition Failure

□ Hide sensor

Filter By Group

Description: The bluetooth driver has failed to add a device. Use Resolve to connect to a system experiencing this issue and investigate for a root cause.

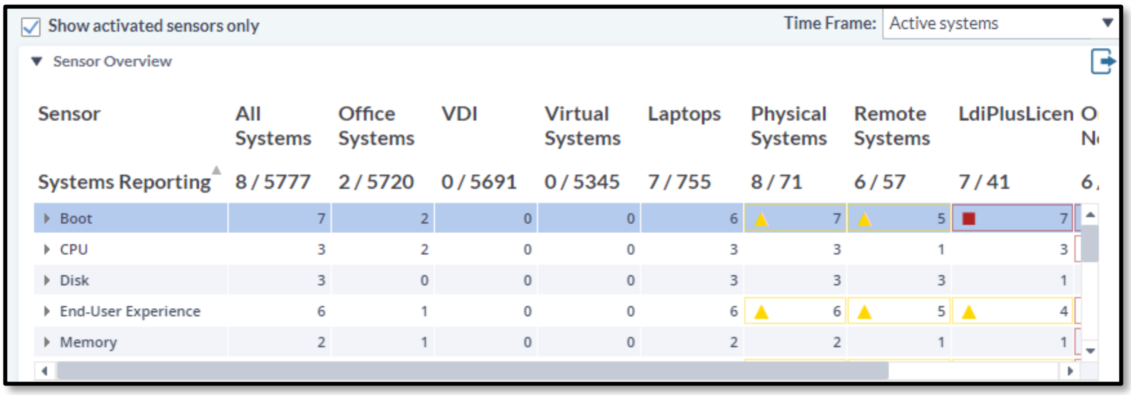
Note: This sensor has no active note.

Sensor Overview Graph

In the Overview module, the Sensor Overview Graphic shows the most pertinent information about any sensors you have enabled.

The first column shows all systems reporting and can be expanded to see each individual sensor being tripped in each category. Double-click the name of the sensor to be taken to the Sensor Details module for more information on data for all systems.

For each column, a red color means that more than 10% of systems are reporting a tripped sensor. A yellow color means more than 5% of systems are reporting a tripped sensor.



☑ Show activated sensors only

Time Frame: Active systems

Sensor	All Systems	Office Systems	VDI	Virtual Systems	Laptops	Physical Systems	Remote Systems	LdiPlusLicen	O N
Systems Reporting	8 / 5777	2 / 5720	0 / 5691	0 / 5345	7 / 755	8 / 71	6 / 57	7 / 41	6,
Boot	7	2	0	0	6	▲ 7	▲ 5	🟥 7	
CPU	3	2	0	0	3	3	1	3	
Disk	3	0	0	0	3	3	3	1	
End-User Experience	6	1	0	0	6	▲ 6	▲ 5	▲ 4	
Memory	2	1	0	0	2	2	1	1	

Discover & Resolve Datasets Overview

Provides an overview of what sensors are being triggered most frequently or have been triggered most recently. By default, you only see sensors that are currently activated.

De-select **Show activated sensors only** to see all sensors being monitored. Use the **Time Frame** drop-down menu to see the latest results for every system, including those not in use.

Sensor Details

This page enables you to drill down into more detailed information about a sensor and why it is activating. You can arrive at this page by double-clicking a sensor from any table containing sensors in Discover & Resolve. You can also select the category and sensor to view the details for any sensor. Make notes on sensors using the notes field.

System Details

Provides information about sensors for a specific system, including a list of sensors being triggered, severity level, and description. Adjust the time frame to see when sensor triggers took place and view a graph of the trending history on that individual system.

Sensor Patterns

Provides a method for identifying patterns in sensor combinations that are happening throughout the environment by correlating sensors with problem users. View the number of sensors occurring on systems and identify if problems need investigating or are localized.

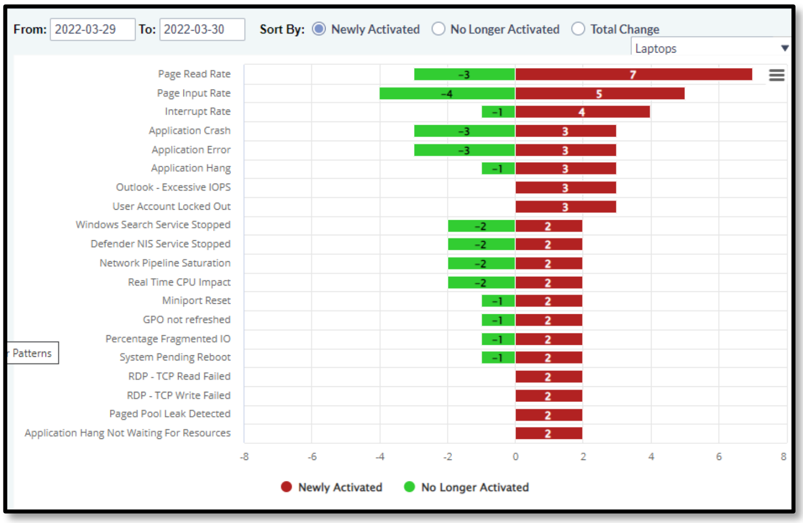
The table lists the groups of sensors that are activating simultaneously. You can see the number of sensors in the pattern, and the number of systems affected by that combination of sensors. This way, you can note whether a sensor pattern is activating rarely on a few machines or if there is a more systemic problem. For example, if the **Sensor Count** is high but **System Count** is low, those sensors are only activating on a few systems, meaning that the problem is localized, whereas if there's a large **System Count**, there's a bigger problem that needs investigating. The average severity shows the severity of the sensors in the given pattern. The Sensors table is sorted by a combination of sensor count, system count, and severity, which displays the most important sensor patterns first.

The next table on the page displays a breakdown of the sensors selected in the first SensorPatterns table, with the severity and description of each sensor.

The Systems section displays the systems that have the selected activated sensor patternand their details, along with charts to visualize the systems. The charts that are one solid color mean that all the systems with the selected pattern have the same value for that attribute. There’s one value in each category for each system experiencing the pattern.

Sensor Trends

Displays the number of systems that have had sensors become activated or deactivated within a certain time range.



From: 2022-03-29 To: 2022-03-30 Sort By: ● Newly Activated ○ No Longer Activated ○ Total Change

Laptops

Red bars indicate the number of systems that have the given sensor activated on the selected end date in the **To** field but did not have the sensor activated on the selected startdate in the **From** field. These are systems where the sensor is newly active in the given timeframe.

Green bars indicate the number of systems that had the given sensor activated on the selected start date in the **To** field but did not have the sensor activated on the selected enddate in the **From** field. These are systems where the sensor has been resolved in the selected time frame.

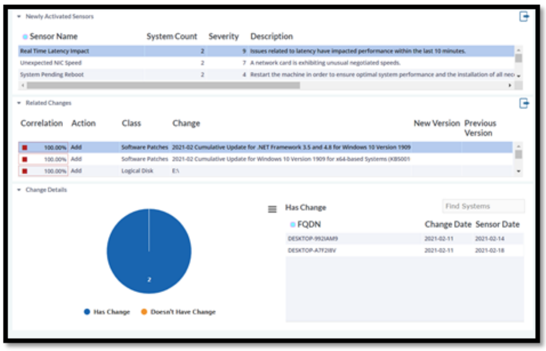
If you select the **Newly Activated** Sort By option, the top sensors will display basedon the number of systems that are newly active (red) in the selected time frame.

If you select the **No Longer Activated** Sort By option, the top sensors will displaybased on the number of systems that sensor has been resolved on (green) in theselected time frame.

If you select the **Total Change** Sort By option, the top sensors will display based onthe total number of systems (red + green) that have experienced a change in the sensor state during the selected time frame.

Root Cause Analysis

Displays changes in the environment that may have caused a sensor to become activated. When you select a sensor in the Newly Activated Sensors table, the Related Changes table below it displays what changes were occurring in the environment shortly before the given sensor was activated. The higher the percentage in the Correlation column, the more likely that the change correlates to the sensor activating.



Newly Activated Sensors

Sensor Name	System Count	Severity	Description
Real Time Latency Impact	2	9	Issues related to latency have impacted performance within the last 10 minutes.
Unexpected NIC Speed	2	7	A network card is exhibiting unusual negotiated speeds.
System Pending Reboot	2	4	Restart the machine in order to ensure optimal system performance and the installation of all nec

Related Changes

Correlation	Action	Class	Change	New Version	Previous Version
100.00%	Add	Software Patches	2021-02 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 1909		
100.00%	Add	Software Patches	2021-02 Cumulative Update for Windows 10 Version 1909 for x64-based Systems (KB5001		
100.00%	Add	Logical Disk	E:\		

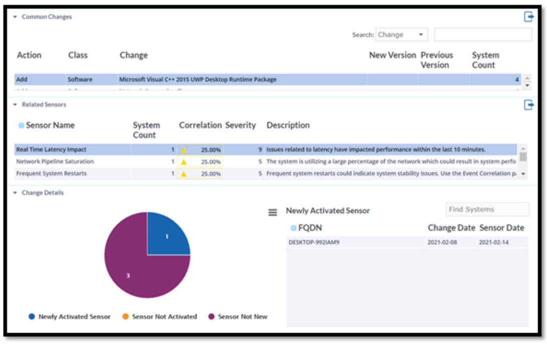
Change Details

Has Change

FQDN	Change Date	Sensor Date
DESKTOP-992IAM9	2021-02-11	2021-02-14
DESKTOP-A7F2I8V	2021-02-11	2021-02-18

Adverse Impact of Changes

Provides an assessment of if any recent changes made are causing sensors to be triggered. Select changes made on the first graph to see which sensors were tripped around that same time.



Common Changes

Search: Change

Action	Class	Change	New Version	Previous Version	System Count
Add	Software	Microsoft Visual C++ 2015 UWP Desktop Runtime Package			4

Related Sensors

Sensor Name	System Count	Correlation	Severity	Description
Real Time Latency Impact	1	25.00%	9	Issues related to latency have impacted performance within the last 10 minutes.
Network Pipeline Saturation	1	25.00%	5	The system is utilizing a large percentage of the network which could result in system perfo
Frequent System Restarts	1	25.00%	5	Frequent system restarts could indicate system stability issues. Use the Event Correlation p

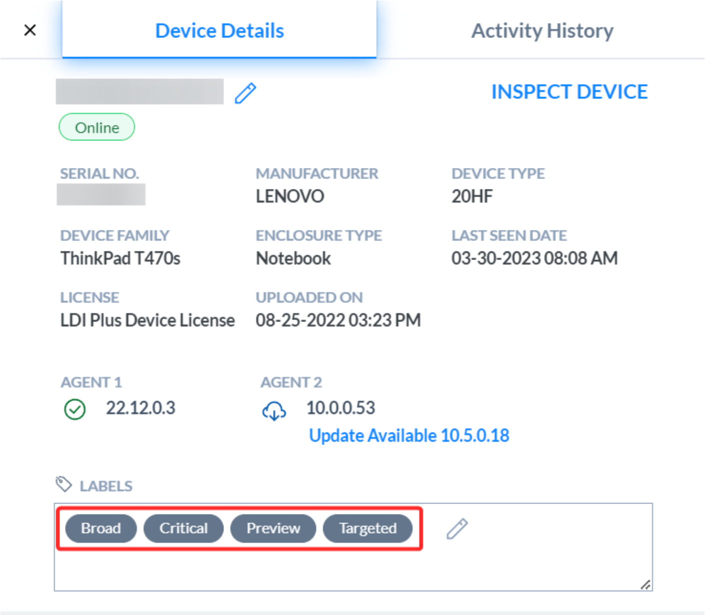
Change Details

Newly Activated Sensor

FQDN	Change Date	Sensor Date
DESKTOP-992IAM9	2021-02-08	2021-02-14

Evergreen IT Control Panel

If you are using Windows Evergreen functionality in your company, you can also monitor how sensors are working on machines that are in different stages of deployment. In order to use the Evergreen IT Control Panel, you will need to define *Preview*, *Targeted*, *Broad*, and *Critical* labels in Device Manager.



[redacted]

SERIAL NO.
[redacted]

MANUFACTURER
LENOVO

DEVICE TYPE
20HF

DEVICE FAMILY
ThinkPad T470s

ENCLOSURE TYPE
Notebook

LAST SEEN DATE
03-30-2023 08:08 AM

LICENSE
LDI Plus Device License

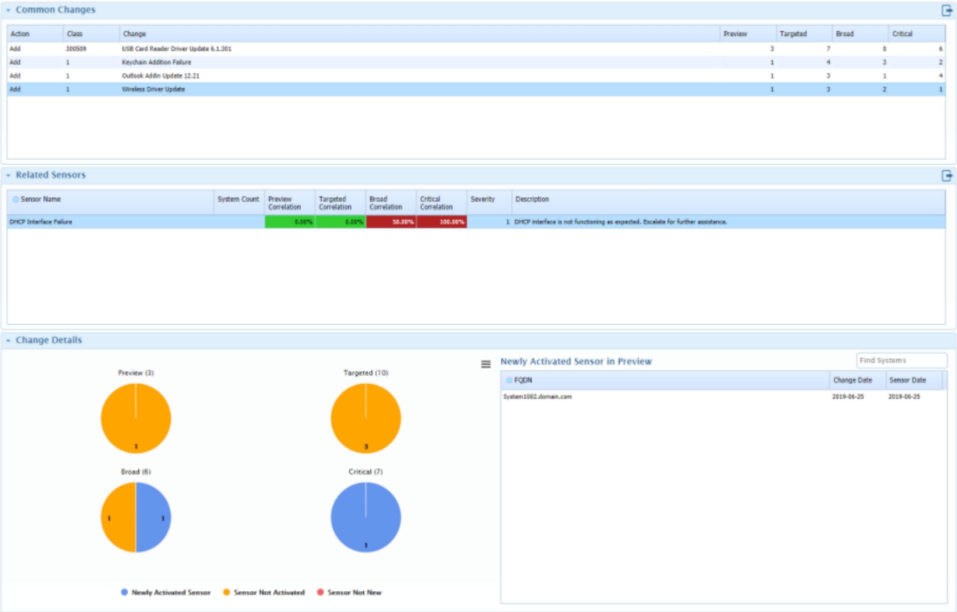
UPLOADED ON
08-25-2022 03:23 PM

AGENT 1
✓ 22.12.0.3

AGENT 2
10.0.0.53
Update Available 10.5.0.18

LABELS
Broad Critical Preview Targeted

If you are not using Evergreen and/or don't have it set up in labels, you will not see this page on the left menu under Discover & Resolve. This page is similar to the Adverse Impact of Changes page except that it is sorted and categorized by Evergreen IT rings.



Common Changes

Action	Class	Change	Preview	Targeted	Broad	Critical
Add	300509	USB Card Reader Driver Update 6.1.301	3	7	8	6
Add	1	Keychain Addition Failure	1	4	3	2
Add	1	Outlook Addin Update 12.21	1	3	1	4
Add	1	Wireless Driver Update	1	3	2	1

Related Sensors

Sensor Name	System Count	Preview Correlation	Targeted Correlation	Broad Correlation	Critical Correlation	Severity	Description
DHCP Interface Failure		0.00%	0.00%	50.00%	100.00%	1	DHCP interface is not functioning as expected. Escalate for further assistance.

Change Details

Newly Activated Sensor in Preview

Find Systems

FQDN	Change Date	Sensor Date
System1002.domain.com	2019-06-25	2019-06-25

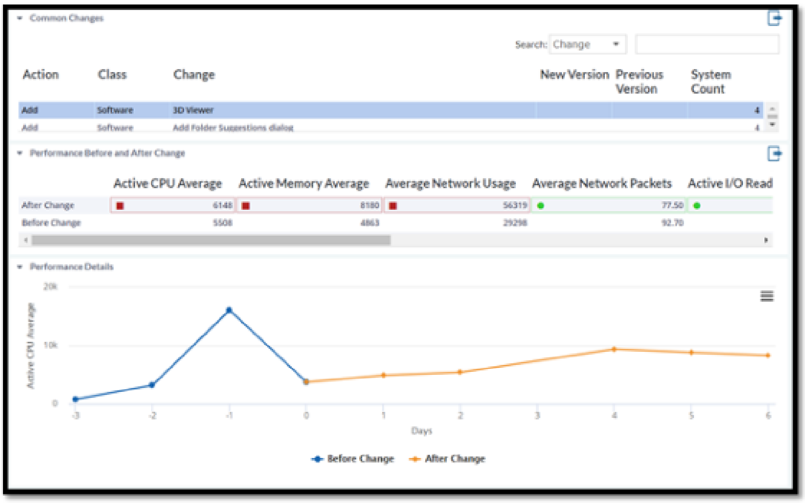
Change Performance

Assesses the performance impact of changes made across many computer systems. You can:

Select a change in the Common Changes table and view a set of performance metrics on the systems that have that change.

View the summary metrics in the week before and after the change in the Performance Before and After Change table.

View the daily average of all systems before and after the change for a selectedmetric in the Performance Details chart.



Common Changes

Search: Change

Action	Class	Change	New Version	Previous Version	System Count
Add	Software	3D Viewer			4
Add	Software	Add Folder Suggestions dialog			4

Performance Before and After Change

	Active CPU Average	Active Memory Average	Average Network Usage	Average Network Packets	Active I/O Read
After Change	🟥 6148	🟥 8180	🟥 56319	● 77.50	●
Before Change	5508	4863	29298	92.70	

Performance Details

Tracking Changes Across Systems

Discover & Resolve runs on each system being monitored and records changes made to individual systems. You can view these changes in the **Common Changes** table.

The data is grouped by type, class, and description to give an overall count of the number of monitored systems that had any given change at any point in the past 30 days. You can search for a specific **Change** or **Class** in the upper-right search bar.

Performance Impact for a Specific Change

When you select a change in the Common Changes table, LDI Plus takes all the daily performance data for every system that has the selected change and time shifts that performance data so that the day of the change is considered Day 0. The day after the change on each system–which could be a different calendar day for any given system–is considered Day 1, the second day after the change is Day 2, and so on. The first day before the change is considered Day -1, the day before that is Day -2, and so on. In this way, LDI Plus can calculate aggregate performance metrics across multiple systems that have a specific change occurring on disparate days.

LDI Plus only considers daily performance records for systems that had at least one active user session during the day. If the system is unused in a particular day, the performance record for that day is ignored.

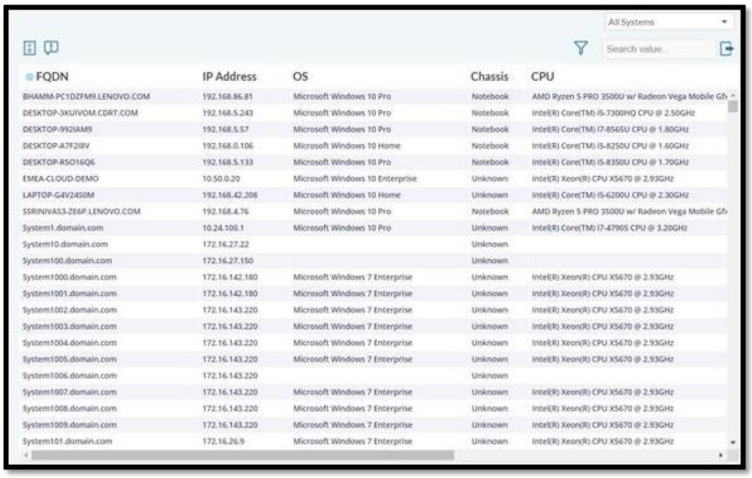
LDI Plus calculates before average for each metric on Days -6 through 0, and an after average for each metric on Days 0 through +6. This allows a high-level comparison of overall system performance before and after the selected change.

For each individual performance metric, you can investigate the daily trend over the covered period.

Tools

Provides the ability to perform an action on a group of systems. First, select a group from the drop-down list in the upper right corner of the page. You can filter the systems down to the systems you want to affect by entering text specific to those systems in the Filter field. The resulting systems that display in the table are affected.

Note: You can only perform actions on systems that are connected to the master system. If a system is not currently connected to the master, it does not receive the action.



FQDN	IP Address	OS	Chassis	CPU
BHAMM-PC1DZFM9.LENOVO.COM	192.168.86.81	Microsoft Windows 10 Pro	Notebook	AMD Ryzen 5 PRO 3500U w/ Radeon Vega Mobile Gfx
DESKTOP-3KUIVOM.CDRT.COM	192.168.5.243	Microsoft Windows 10 Pro	Notebook	Intel(R) Core(TM) i5-7300HQ CPU @ 2.50GHz
DESKTOP-992IAM9	192.168.5.57	Microsoft Windows 10 Pro	Notebook	Intel(R) Core(TM) i7-8565U CPU @ 1.80GHz
DESKTOP-A7F2I8V	192.168.0.106	Microsoft Windows 10 Home	Notebook	Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz
DESKTOP-RSO16Q6	192.168.5.133	Microsoft Windows 10 Pro	Notebook	Intel(R) Core(TM) i5-8350U CPU @ 1.70GHz
EMEA-CLOUD-DEMO	10.50.0.20	Microsoft Windows 10 Enterprise	Unknown	Intel(R) Xeon(R) CPU X5670 @ 2.93GHz
LAPTOP-G4V2450M	192.168.42.208	Microsoft Windows 10 Home	Unknown	Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz
SSRINIVAS3-ZE6P.LENOVO.COM	192.168.4.76	Microsoft Windows 10 Pro	Notebook	AMD Ryzen 5 PRO 3500U w/ Radeon Vega Mobile Gfx
System1.domain.com	10.24.100.1	Microsoft Windows 10 Pro	Unknown	Intel(R) Core(TM) i7-4790S CPU @ 3.20GHz
System10.domain.com	172.16.27.22		Unknown	
System100.domain.com	172.16.27.150		Unknown	
System1000.domain.com	172.16.142.180	Microsoft Windows 7 Enterprise	Unknown	Intel(R) Xeon(R) CPU X5670 @ 2.93GHz
System1001.domain.com	172.16.142.180	Microsoft Windows 7 Enterprise	Unknown	Intel(R) Xeon(R) CPU X5670 @ 2.93GHz
System1002.domain.com	172.16.143.220	Microsoft Windows 7 Enterprise	Unknown	Intel(R) Xeon(R) CPU X5670 @ 2.93GHz
System1003.domain.com	172.16.143.220	Microsoft Windows 7 Enterprise	Unknown	Intel(R) Xeon(R) CPU X5670 @ 2.93GHz
System1004.domain.com	172.16.143.220	Microsoft Windows 7 Enterprise	Unknown	Intel(R) Xeon(R) CPU X5670 @ 2.93GHz
System1005.domain.com	172.16.143.220	Microsoft Windows 7 Enterprise	Unknown	Intel(R) Xeon(R) CPU X5670 @ 2.93GHz
System1006.domain.com	172.16.143.220		Unknown	
System1007.domain.com	172.16.143.220	Microsoft Windows 7 Enterprise	Unknown	Intel(R) Xeon(R) CPU X5670 @ 2.93GHz
System1008.domain.com	172.16.143.220	Microsoft Windows 7 Enterprise	Unknown	Intel(R) Xeon(R) CPU X5670 @ 2.93GHz
System1009.domain.com	172.16.143.220	Microsoft Windows 7 Enterprise	Unknown	Intel(R) Xeon(R) CPU X5670 @ 2.93GHz
System101.domain.com	172.16.26.9	Microsoft Windows 7 Enterprise	Unknown	Intel(R) Xeon(R) CPU X5670 @ 2.93GHz

IT Announcements

Provides the ability to create the IT announcements that display in the IT Self Help App. Click the **Add** + icon, enter the Announcement, click the **Calendar** 📅 icon when you want the announcement to stop displaying in the app, and click **OK**. You can also edit and delete these announcements.

4.4 User Experience

4.4.1 Fleet Overview

4.4.1.1. Dashboard

The User Experience dashboard module provides a quality measurement system that puts CIOs, administrators, and help desk technicians on the same page by providing a uniform system that promotes role-appropriate views on a common data mine.

User Experience includes the following dashboard modules:

Fleet Overview

Provides CIOs with a real-time view that is happening within key organizational groups across the entire computing landscape.

Device Overview

Provides an IT manager perspective of specific systems and users with more in-depth problem diagnostics.

Risk Analysis

Provides views to assist in identifying areas of potential security risk, including details of application configurations and inventory, hardware and system configurations, and installed packages.

Persona Analysis

Provides abstract models of real users based on work patterns, behaviors, and tools of actual users in the environment. Personas allow IT to distil users1 down to a manageable number of user types and understand what a persona requires from a hardware, software, mobility, security, and software perspective. Knowing these requirements aids in effectivelyprovisioning support resources, including budget and personnel, to maximize the end user experience.

Sector Benchmarks

Sector Benchmarks allows LDI Plus customers to compare key performance indicators (KPIs) from their environment to a representative sample of peer data from other organizations. Peer benchmarking is also helpful for assessing whether your IT environment is at a competitive advantage or disadvantage. While internal benchmarking is important for measuring improvements withing your own environment over time, external benchmarkingenables you to assess your success in a broader context. Access to industry averages can help a customer build a better case for increased attention or investments to improve.

Organizations can also answer questions like How is everyone else doing? Each dashboard module contains its own menu to categorize datasets as needed. Hover over the names of the menu items to learn more about what each can do.

Navigate the Dashboard Modules

Each dashboard module provides unique information pertaining to the particular view available in a set of adjustable cards across the page.

⤓ - If a card contains this icon, you can export the data to a spreadsheet.

? - If a card contains this icon, you can click on it to learn more about the data in that area.

Some cards may be expandable. Hovering over an expandable card causes a small triangle to appear in the lower right corner. You can click and drag the arrow to resizethe cards for better data viewing.

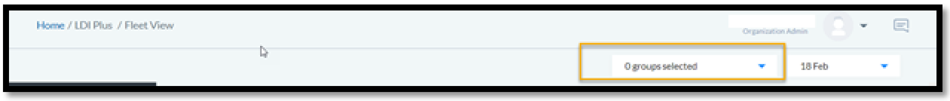
Cards may also be reordered to suit your needs. Hovering over a card near the edges causes a multi-directional arrow to appear. Click this arrow to drag and drop a card and re-order the displayed cards.

On some dataset displays, different cards may be collapsible. If the title of the card is preceded by a downward or upward pointing arrow, the card may be collapsed or expanded.

Detail Bar

Some modules may include a detail bar slider at the bottom of the menu. Use this slider to change the amount of detail visible to different users.

Select a Group

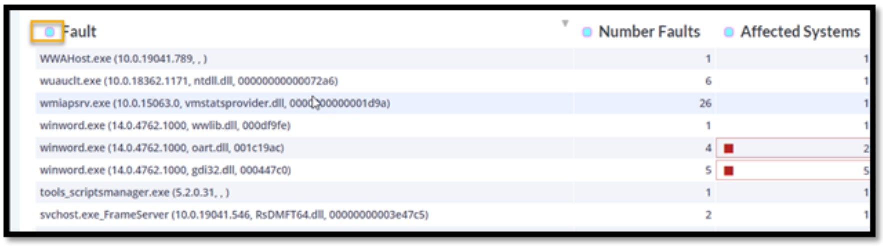


If you have a large site, you may find it convenient to review data for smaller groups within your site, rather than view data for all systems (which is the default). Groups provide this mechanism. Once this is done, you can then select a specific group from the menu to filter the data displayed to just that group.

Get More Detail

A blue dot in any column of a grid means you can double-click on an item in that column for more detail.

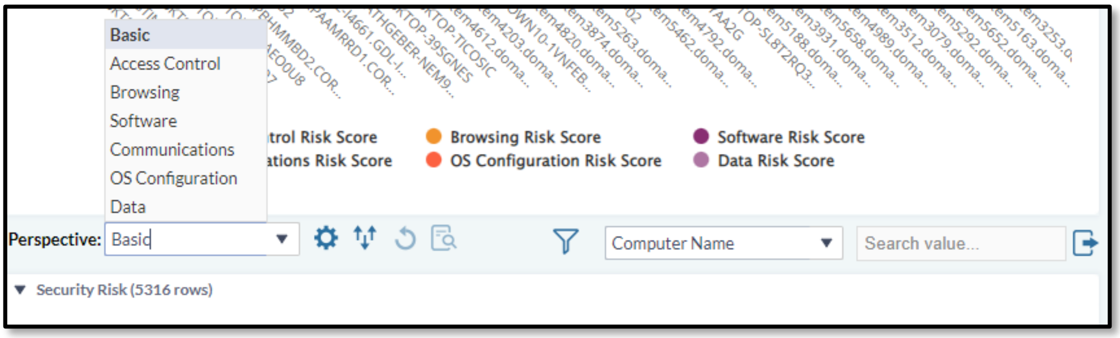
Note: You may be taken to a different section of LDI Plus after double clicking on an item. To return to the starting location, click the back button on your browser.



● Fault	● Number Faults	● Affected Systems
WWAHost.exe (10.0.19041.789, ,)	1	1
wuauclt.exe (10.0.18362.1171, ntdll.dll, 00000000000072a6)	6	1
wmiapsrv.exe (10.0.15063.0, vmstatsprovider.dll, 0000000000001d9a)	26	1
winword.exe (14.0.4762.1000, wwlib.dll, 000df9fe)	1	1
winword.exe (14.0.4762.1000, oart.dll, 001c19ac)	4	🟥 2
winword.exe (14.0.4762.1000, gdi32.dll, 000447c0)	5	🟥 5
tools_scriptsmanager.exe (5.2.0.31, ,)	1	1
svchost.exe_FrameServer (10.0.19041.546, RsDMFT64.dll, 00000000003e47c5)	2	1

Perspectives

Perspectives allow users to view datasets in different ways, isolating information to show specific results that may aid in understanding different situations. Each dataset has a unique set of Perspectives available, depending on the type of data displayed.



Perspective: Basic

Security Risk (5316 rows)

Note: Some datasets may only have the Basic Perspective available.

4.2.1.1. Application Faults

Provides an assessment of how problems of Fleet View present the CIO or IT Director with an objective, high-level view of what is happening across the computing enterprise, providing visibility into the end-user computing landscape that has traditionally been largely unmanaged. To optimize the computing environment, increase end-user satisfaction, and drive down costs, one needs critical information about the underlying systems and applications. These include, but are not limited to, reporting on end user quality, concurrent usage, software packages, system performance, resource utilization and security.

The Fleet View dashboard provides a graphical aggregate view of the enterprise environment that allows you to quickly see how the metrics are trending. To enable this view, click **User Experience**, and then select **Fleet View** from the main menu. The applications may impact the users in the community being analysed.

Applications, the executable components of software packages, may fault due to application programming errors, environmental issues, resource constraints, and other causes. Such faults can have a serious impact on user productivity, user satisfaction with the IT environment, and the overall user experience. Each application fault detected is analysed and categorized by its type and underlying cause. This information may assist the IT architect to identify and resolve the underlying cause of the fault and may additionally help distinguish application faults that are (or are not) the result of changes made in the application delivery infrastructure.The Application Faults dataset provides the following perspectives:

Basic

This perspective summarizes application faults detected on systems during the observation period. Faults are analysed and categorized according to their cause. This overview may help the IT architect to focus resources on problematic applications that affect the largest part of the user community.

Faults Affecting Multiple Systems

This perspective shows application faults that were detected on more than one computer system. Faults are analysed and categorized according to their cause. Faults that occur on more than one system are likely to indicate software problems as opposed to isolated user configurations and behaviors.

Fault Technical Details

This perspective provides the full technical details for each category of faults detected. Information provided here may be helpful to software developers in resolving specific problems.

Application Hangs

This perspective shows those application faults that were manifested to the user as a hang of the respective application. Such faults are indicative of a class of faults that may be more difficult to isolate and resolve due to the lack of a specific crash dump. Applications with high application hang counts are often associated with user frustration due to the poor quality of the end user experience.

Application Crashes

This perspective shows those application faults that were manifested to the user as a crash of the respective application. It is possible to configure the computer system on which these crashes occur such that a crash dump file is automatically generated. Such crash dump files make debugging and fault resolution by the application developer much easier.

Troubled Applications

Applications in the upper right quadrant are causing high amounts of productivity loss in the enterprise and may need of patching, upgrade, or further investigation.

4.2.1.2. Application Virtualization

Depicts the extent to which software packages that are presently in use may be compatible with application virtualization technology. Application Virtualization allows software packages to be packed and delivered to the user in a way that minimizes or eliminates installation procedures and facilitates delivery of desktops through desktop pools. Compatibility with application virtualization may influence the design of application delivery environments, enabling new efficiencies that reduce the total cost of ownership. Each software package in the visualized environment is analysed for specific attributes that may complicate or preclude delivery of the application through virtualization technology. This information may assist the IT architect in designing the computing environment in a way that delivers needed software packages using the lowest cost and lowest impact methodology.

The Application Virtualization dataset contains multiple perspectives:

Basic

This perspective provides a high-level view of the extent to which application virtualization technologies may be successfully leveraged. Application virtualization may offer substantial benefits in reduction of administrative costs and promoting desktop pooling among the user community but may be limited in certain cases by specific attributes of the software packages in use.

Packages Already Virtualized

This perspective identifies software packages that have been identified in the environment as being delivered through application virtualization on one or more systems. Note that any application virtualization concerns identified may have eitherbeen avoided through specific techniques or may have been ignored at the loss of some functionality, which may or may not be significant to the user experience.

Virtualization Concern Details

This perspective shows the detailed application virtualization concerns that must be considered for each software package during the design and qualification phase.

Packages with Device Drivers

This perspective identifies software packages that contain one or more services. Suchsoftware packages may require special consideration if they are to be delivered through application virtualization.

Packages with Office Add-ins

This perspective identifies software packages that contain one or more Microsoft Office Add-in components. Such software packages may require special consideration if they are to be delivered through application virtualization.

Packages with IE Extensions

This perspective identifies software packages that contain one or more Internet Explorer extensions. Such software packages may require special consideration if they are to be delivered through application virtualization.

Packages with IE Toolbars

This perspective identifies software packages that contain one or more Internet Explorer Toolbars. Such software packages may require special consideration if theyare to be delivered through application virtualization.

Packages with Shell Extensions

This perspective identifies software packages that contain one or more Windows shellextensions. Such software packages may require special consideration if they are to be delivered through application virtualization.

Packages with 16-bit Components

This perspective identifies software packages that contain one or more 16-bit components. Such software packages may require special consideration if they are tobe delivered through application virtualization.

Candidates for Application Virtualization

Packages in the upper left may be good candidates for virtualization as they have the fewest concerns and have the greatest impact to the enterprise.

4.2.1.3. Applications

Provides insight into the behavior and use of applications, which are the executable components of software packages. In contrast to software packages, which often represent purchasable and installable bundles of applications, applications are the individual executable components that consume resources on computers.

Each application in the visualized community is statistically analysed and presented in the dataset with key performance indicators that may be helpful in planning the IT environment. These statistics help the IT architect to understand the resources demanded by applications for optimal performance, how the behavior of these applications may impact the user experience, and usage profile information that helps depict user communities that are made more productive using these applications.

The Applications dataset contains multiple perspectives:

Basic

This perspective delivers a high-level view of the applications used. For each application, key metrics that indicate the typical, overall resource consumption of the application along with usage data that helps qualify how it is used are shown.

CPU Technical Analysis

This perspective provides deeper technical data regarding CPU consumption by eachapplication. Statistical data offered here promotes a finer level of understanding of the processor resource utilization for each application.

Memory Technical Analysis

This perspective provides deeper technical data regarding memory consumption by each application. Statistical data offered here promotes a finer level of understanding of the memory resource requirements for each application.

I/O Technical Analysis

This perspective provides deeper technical data regarding disk I/O consumption by each application. Statistical data offered here promotes a finer level of understanding of the I/O behavior of each application.

Usage Summary

This perspective further qualifies how applications are used. More detailed data regarding usage patterns may be helpful in planning support for these applications.

Application Start-up Experience

This perspective offers insight into the start-up delay experienced by users of the application. While some applications inherently require more time to start due to processing requirements during the load sequence, statistical measurements offered here may help to depict typical delays expected in this environment for each application.

Application Workload Details

Data delivered in this perspective helps to size the overall workload presented by a package as operated by the community. Detailed technical data shown here clarifies how a particular application presents a workload for the computing environment on which it runs.

Configuration Details

This perspective provides an analysis of the GPU and video support requirements, the Microsoft .NET framework requirements, and the Microsoft run time libraries that are required by each application.

Heavily Used Applications

Applications presented in this perspective are presented in order of usage intensity to provide a high-level overview of what drives the most activity.

Applications in Need of Standardization

Applications are easiest to support when only one version exists in the enterprise. In this graph, applications found in the upper right quadrant are those that are in use by many users and where many versions exist. Standardizing on one version of these applications has the greatest impact to productivity and stability in the environment, while reducing support costs.

Network

Provides deeper technical data regarding the network usage by each application.

4.2.1.4. Software Packages

Provides insight into the behavior and use of software packages, which are collections of applications. Software packages are generally purchasable and installable bundles that consume resources when the contained applications areaccessed.

The Software Packages dataset provides the following perspectives:

Basic

This perspective delivers a high-level view of the software packages used in the visualized community. For each software package, key metrics that indicate the typical, overall resource consumption of the software package along with usage datathat helps qualify how it is used are shown.

CPU Technical Analysis

This perspective provides deeper technical data regarding CPU consumption by eachsoftware package. Statistical data offered here promotes a finer level of understanding of the processor resource utilization for each software package.

Memory Technical Analysis

This perspective provides deeper technical data regarding memory consumption byeach software package. Statistical data offered here promotes a finer level of understanding of the memory resource requirements for each software package.

I/O Technical Analysis

This perspective provides deeper technical data regarding disk I/O consumption byeach software package. Statistical data offered here promotes a finer level of understanding of the I/O behavior of each software package.

Usage Summary

This perspective further qualifies how software packages are used in the visualizedenvironment. More detailed data regarding usage patterns may be helpful in planning support for these software packages.

Package Workload Details

Data delivered in this perspective helps to size the overall workload presented by asoftware package as operated by the community. Detailed technical data shown here clarifies how a particular software package presents a workload for the computing environment on which it runs.

Named User vs. Per Device licensing

This perspective helps the IT architect to select application licensing modes that aremost economically efficient. Available licensing models vary widely by application, but this perspective helps to contrast the use of software packages by named usersversus systems on which the application may be installed.

Configuration Details

This perspective provides an analysis of the GPU and video support requirements,the Microsoft .NET framework requirements, and the Microsoft run time librariesthat are required by each software package.

Unused Software

This perspective provides an analysis of software packages that are installed on systems but are potentially unused. Different columns reflect the period over whichno use has been detected. In most cases, software licensing and maintenance costs can be reduced by minimizing the amount of unused software in the visualized environment.

Usage Detail

This perspective provides details of usage patterns for software packages. Differentcolumns reflect the number of systems on which the software was installed, the number of systems on which the software package was used, the number of user accounts that used the software package, the estimated accuracy of the usage datadisplayed, and the number of systems by period over which no use has been detected.

Systems Installed vs. Used

This perspective shows how the number of systems installed compares with thenumber of users of the system for each software package.

Usage Data Accuracy

This perspective shows how the accuracy of the software usage detection algorithmvaries with the number of installed systems for each software package.

Unused Software: 30 Days

This perspective shows how the number of instances of the software package thathave been unused for the past 30 days compares with the total number of installations of the software package.

Unused Software: 60 Days

This perspective shows how the number of instances of the software package thathave been unused for the past 60 days compares with the total number of installations of the software package.

Unused Software: 90 Days

This perspective shows how the number of instances of the software package thathave been unused for the past 90 days compares with the total number of installations of the software package.

Software Package CPU/MEM Usage

Software packages that consume the most resources when in use have the greatest impact to the IT infrastructure overall especially when virtualized. These applications require the greatest amount of CPU and memory resources.

Software Package Disk/SAN Usage

Software packages that produce the most data can be found on the far right of this graph. Those near the top are those that consume the most data. Software Packages found in the upper left are those that may benefit the most from SAN implementation for the data storage. These packages benefit from IO read cached appliances because the applications read similar data across the enterprise. You can do group versus group data comparison. You can use this tool to gain a better understanding of the system or group is performing versus others, using nearly all the data available with LDI Plus. The columns available for graphing have further detail when you hover over them.

4.2.1.5. Analysis

The Analysis feature helps you analyse data using the following tabs:

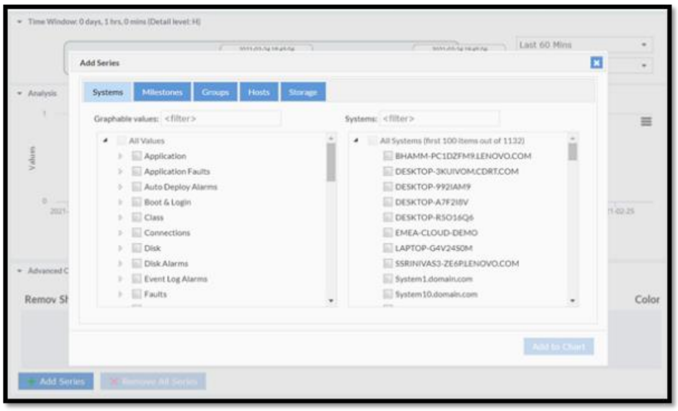
Systems - System versus system metric graphing comparison

Milestones - Historic event graphing of alarms, events, sensors, and more

Groups - Group versus group metric graphing comparison

Hosts - Server versus server metric graphing comparison

Storage - Disk space graphing



While the Fleet View module provides an executive-level picture, the Device Overview module presents a more detailed IT Manager perspective of specific systems and users, providing more in-depth problem diagnostics.

The Device View module allows you to drill-down to the individual user, system, and application level. Besides end-user experience reporting, both the Fleet View and Device View modules provide sets of data for software packages, applications, system performance, security, systems, latency, power, storage, application virtualization, and fault management.

4.2.2 Device Overview

4.2.2.1. Dashboard

Provides an overview of information available in the Device Overview.

4.2.2.2. Application Faults

Basic

Provides an assessment of how problems with applications may impact the users in the group being analysed.

Application Faults

This perspective summarizes application faults detected on systems during the observation period. Faults are analysed and categorized according to their cause. This overview may help an IT architect focus resources on problematic applications that affect the largest part of the user community.

Faults Affecting Multiple Systems

This perspective shows application faults that were detected on more than one computer system. Faults are analysed and categorized according to their cause. Faults that occur on more than one system are likely to indicate software problems as opposed to isolated user configurations and behaviors.

Fault Technical Details

This perspective provides the full technical details for each category of fault detected. Information provided here may be helpful to software developers in resolving specific problems.

Application Hangs

This perspective shows those application faults that were manifested to the user as a hang of the respective application. Such faults are indicative of a class of faults that may be more difficult to isolate and resolve due to the lack of a specific crash dump. Applications with high application hang counts are often associated with user frustration due to the poor quality of the end user experience.

Application Crashes

This perspective shows those application faults that were manifested to the user as a crash of the respective application. It is possible to configure the computer system on which these crashes occur such that a crash dump file is automatically generated. Such crash dump files make debugging and fault resolution by the application developer much easier.

Troubled Applications

Applications in the upper right quadrant are causing high amounts of productivity loss in the enterprise and may need of patching, upgrade, or further dataset.

4.2.2.3. Application Latency

Provides information about which applications have dependencies on external servers anddata sources, how such dependencies may align with the needs of other applications and systems, and how delays inherent in the network communications design may impact the end user experience of users in the community.

The Application Latency provides the following dataset perspectives:

Basic

This perspective delivers a high-level view of networked applications and their dependencies on target servers. Systems on which these applications execute areorganized by their target server, and rows depict typical measured latency from those subnets to the target server for the specified application.

Technical Detail by Subnet

This perspective offers greater technical detail in depicting latency experienced by networked applications in communicating with dependent servers. Statistical data enhances the understanding of the behavior of underlying networks. The standard deviation of latency helps quantify the range of latency experienced on the specifiedconnection. Latency is statistically analysed by samples of computers on the source subnet.

Technical Detail by System Samples

This perspective offers greater technical detail in depicting latency experienced by networked applications in communicating with dependent servers. Statistical data enhances the understanding of the behavior of underlying networks. The standard deviation of latency helps qualify the range of latency experienced on the specified connection. Latency is statistically analysed by of individual latency samples taken onthe source subnet.

Latency by Source Subnet

This perspective delivers a high-level view of networked applications and their dependencies on target servers. Systems on which these applications execute are organized by their source subset, and rows depict typical measured latency from those subnets to the target server for the specified application.

Latency to Default Gateway

This perspective delivers a high-level view of networked applications and their dependencies on target servers. Systems on which these applications execute are organized by their source subnet, and rows depict typical measured latency from those subnets to the target server for the specified application.

Application Server Latency

This perspective shows the latency from each source subnet to the default gateway for that subnet. Since most network traffic from computers traverses the default gateway, ensuring minimal latency here may be particularly helpful to overall performance.

4.2.2.4. Application Virtualization

Depicts how the Software Packages are compatible with Application Virtualization technology.

The Application Virtualization dataset contains the following perspectives:

Basic

This perspective provides a high-level view of the extent to which application virtualization technologies may be successfully leveraged in the visualized environment. Application virtualization may offer substantial benefits in reduction ofadministrative costs and promote desktop pooling among the user community but may be limited in certain cases by specific attributes of the software packages in use.

Packages Already Virtualized

This perspective identifies software packages that have been identified in the environment as being delivered through application virtualization on one or more systems. Note that any application virtualization concerns identified may have eitherbeen avoided through specific techniques or may have been ignored at the loss of some functionality, which may or may not be significant to the user experience.

Virtualization Concern Details

This perspective shows the detailed application virtualization concerns that must beconsidered for each software package during the design and qualification phase.

Packages with Device Drivers

This perspective identifies software packages that contain one or more device drivers. Such software packages may require special consideration if they are to be delivered through application virtualization.

Packages with Services

This perspective identifies software packages that contain one or more services. Such software packages may require special consideration if they are to be delivered through application virtualization.

Packages with Office Add-ins

This perspective identifies software packages that contain one or more Microsoft Office Add-in components. Such software packages may require special consideration if they are to be delivered through application virtualization.

Packages with IE Extensions

This perspective identifies software packages that contain one or more Internet Explorer extensions. Such software packages may require special consideration if they are to be delivered through application virtualization.

Packages with IE Toolbars

This perspective identifies software packages that contain one or more Internet Explorer Toolbars. Such software packages may require special consideration if they are to be delivered through application virtualization.

Packages with Shell Extensions

This perspective identifies software packages that contain one or more Windows shell extensions. Such software packages may require special consideration if they are to be delivered through application virtualization.

Packages with 16-bit Components

This perspective identifies software packages that contain one or more 16-bit components. Such software packages may require special consideration if they are to be delivered through application virtualization.

Packages with 64-bit Components

This perspective identifies software packages that contain one or more 64-bit components. Such software packages may require special consideration if they are to be delivered through application virtualization.

Candidates for Application Virtualization

Packages in the upper left may be good candidates for virtualization as they have the fewest concerns and have the greatest impact to the enterprise.

4.2.2.5. Applications

Provides insight into the behavior and use of applications, which are the executable components of Software Packages.

The Applications dataset provides the following perspectives:

Basic

This perspective delivers a high-level view of the applications used in the visualized community. For each application, key metrics that indicate the typical, overall resource consumption of the application along with usage data that helps qualify how it is used are shown.

CPU Technical Analysis

This perspective provides deeper technical data regarding CPU consumption by eachapplication. Statistical data offered here promotes a finer level of understanding of the processor resource utilization for each application.

Memory Technical Analysis

This perspective provides deeper technical data regarding memory consumption byeach application. Statistical data offered here promotes a finer level of understanding of the memory resource requirements for each application.

I/O Technical Analysis

This perspective provides deeper technical data regarding disk I/O consumption byeach application. Statistical data offered here promotes a finer level of understanding of the I/O behavior of each application.

Usage Summary

This perspective further qualifies how applications are used in the visualized environment. More detailed data regarding usage patterns may be helpful inplanning support for these applications.

Application Startup Experience

This perspective offers insight into the start-up delay experienced by users of the application. While some applications inherently require more time to start due to processing requirements during the load sequence, statistical measurements offeredhere may help to depict typical delays expected in this environment for each application.

Application Workload Details

Data delivered in this perspective helps to size the overall workload presented by a package in the visualized environment as operated by the community. Detailed technical data shown here may clarify how a particularapplication presents a workload for the computing environment on which it runs.

Configuration Details

This perspective provides an analysis of the GPU and video support requirements, the Microsoft .NET framework requirements, and the Microsoft run time librariesthat are required by each application.

Heavily Used Applications

Applications presented in this perspective are presented in order of usage intensityto provide a high-level overview of what drives the most activity in the community.

Applications in Need of Standardization

Applications are easiest to support when only one version exists in the enterprise. Inthis graph, applications found in the upper right quadrant are those that are in use by many users and where many versions exist. Standardizing on one version of theseapplications will have the greatest impact to productivity and stability in the environment, while reducing support costs.

Network

This perspective provides deeper technical data regarding the network usage byeach application.

4.2.2.6. Boot and Login

Provides an indication of the boot and login performance experienced by users.The Boot and Login dataset provides the following perspectives:

Basic

This perspective provides an overview of the boot and login performance of collections of systems. It is helpful in identifying cases here the time required to complete boot and/or login operations has a negative impact on productivity.

Boot Details

This perspective provides details on the operations required to complete the system boot process for collections of systems. The timing for the boot stages shown reflects how long it takes to complete each segment of the boot operation.

Login Details

This perspective provides details on the operations required to complete the logon process for collections of systems. The timing for the login stages shown reflects how long it takes to complete each segment of the login operation.

Profiles and Group Policy

This perspective provides details on profile and group policy processing required to complete the system boot and login processes for collections of systems.

Boot/Login Resources

This perspective provides details on the resources consumed during system boot and login processes for collections of systems.

4.2.2.7. Computer Concerns

Provides an assessment of how hardware that part of the existing computingplatform may impact user needs for future application delivery platforms.

The Computer Concerns dataset provides the following perspectives:

Basic

This perspective identifies specific attributes of computer use and computer device use that may impact the design and delivery of applications to its users. Each computer device in the visualized community is analysed for mobility attributes, local printers, modems, and USB storage device use.

Systems with Mobility Requirements

This perspective identifies those computers that are either potentially used as mobile devices or are observed in mobile use during the observation period. Devices that were not observed in mobile use but have a form factor that would promote such mobility are identified as potentially mobile.

Systems where USB Devices are Used

This perspective identifies those computers on which the user community leverages USB storage devices. Such devices may be used either continuously, or their intermittent use may be detected during the observation period.

Systems with Local Printers

This perspective identifies those computers that have locally attached printers.

Systems with Modems

This perspective identifies those computers that have installed modem devices.

Systems with No Mobility or Device Needs

This perspective enumerates computer systems in the visualized community that are not mobile and have no local printers, modems, or USB devices.

4.2.2.8. Computer Performance

Provides insight into how computers are used and how much of their available compute resources are effectively used in delivering applications to users.

The Computer Performance dataset provides the following perspectives:

Basic

This perspective offers a high-level view of computer performance for systems. For each system, average resource demand for CPU, memory, I/O, and network are shown. The primary user and typical weekly active time (not including screen saver and display lock) are provided, along with the typical time spent each week in graphically oriented applications.

CPU Technical Analysis

This perspective offers deeper technical details regarding the use of processor resources on each computer system. Sizing of virtualized desktops is most influenced by average CPU consumed and the standard deviation of the load during login periods, in which physical desktops may be best sized using the maximum resource consumption and standard deviation.

Memory Technical Analysis

This perspective offers deeper technical details regarding the use of memory resources on each computer system. Statistical data such as the maximum and standard deviation of the workload may be helpful in proper and efficient sizing.

I/O Technical Analysis

This perspective offers deeper technical details regarding the use of I/O resources on each computer system. Statistical data such as the maximum and standard deviation of the workload may be helpful in proper and efficient sizing.

Network Technical Analysis

This perspective offers deeper technical details regarding the use of network resources on each computer system. Statistical data such as the maximum and standard deviation of the workload may be helpful in proper and efficient sizing.

Usage by Login and Active Time

This perspective provides more detailed usage data regarding the use of the computer system by the user community. The primary user and typical login (including screen saver and display lock) and active periods are indicated.

Graphics Acceleration Usage

This perspective provides more detailed usage information about how the workload on each computer system leverages GPU acceleration technologies. Data depicted includes the weekly time spent in applications that make use of video acceleration, which is further divided into use by browser applications and non-browser applications.

Browser Usage

This perspective provides detailed usage information about how much time the usercommunity spends in internet browser applications. Browser usage data is divided into graphical and non-graphical usage subsets, and related information about login time, active time, and graphical application time is also made available.

Unused Computers

This perspective identifies computers for which no logins have been detected. If these computers are not used as servers (for which a lack of login activity is normal),they may potentially be unused systems. In most cases, costs can be reduced by minimizing the number of unused computers in the visualized environment.

System Resource Footprint

Systems that consume the most resources have the greatest impact to the IT infrastructure overall especially when virtualized. These systems found in the upper right require the greatest amount of CPU and memory.

4.2.2.9. Hardware

Provides asset and configuration data that describes the fundamentals of the computing environment delivered to the user.

The Hardware dataset provides the following perspectives:

Basic

This perspective provides a high-level overview of the computer systems. The type ofsystem, hardware or virtualized platform, and overall resource capacity delivered areindicated for each computer.

CPU Details

This perspective provides deeper technical details about the processor resources available from each computing platform.

Video Details

This perspective provides deeper technical details about the video adapter and monitor configuration available from each computing platform.

Operating System Details

This perspective provides deeper technical details about the operating system installed on each computing platform.

Network Details

This perspective provides deeper technical details about the network adapter andconfiguration on each computing platform.

Processor and Memory Capacity

Systems in the upper right of the chart are highest overall capacity when CPU and

memory are factors.

4.2.2.10. Health

Provides an indication of the quality of service delivered to users.

The Health dataset provides the following perspectives:

Basic

This perspective provides an overview of the health of systems and quantifies the productivity impact of any problems identified. The quality time depicts the percentage of active time during which the user's productivity was not impacted by any tracked concern.

Productivity Impact Full Details

This perspective provides the full details regarding the health of systems in the visualized environment and quantifies the productivity impact of any problems identified. For each type of concern, the impact of the problems on user productivity is quantified.

Systems Impacted by Resource Constraints

This perspective provides the details of how resource constraints may impact systems and quantifies the productivity impact of any problems identified.

Systems Impacted by Configuration Issues

This perspective provides the details of how configuration matters may impact systems and quantifies the productivity impact of any problems identified.

Systems Impacted by Software Problems

This perspective provides the details of how software problems such as application crashes and hangs, and system crashes may impact systems and quantifies the productivity impact of any problems identified.

User Experience Quality

This perspective provides an overview of the user experience quality on systems and quantifies the total productivity impact of any problems identified. The quality time depicts the percentage of active time during which the user's productivity was not impacted by any tracked concern.

Systems Experiencing Hardware Issues

Systems experiencing both hardware interrupt issues and system or application faults may be suffering from hardware failures or driver conflicts. The systems most impacted by these concerns are those in the upper right quadrant.

Systems in Need of Maintenance Window

Systems that are performing multiple software installs and updates during user sessions will benefit most from off-hours updates. Systems located in the upper right quadrant of this graph are those that are causing the most user impact.

4.2.2.11. Power

The Power dataset provides the following perspectives:

Energy Consumption Detail

This perspective provides more technical data regarding the energy used to operate each physical computer system. Energy consumed is shown in the average direct electricity consumption in power-on periods, as well as in total energy consumed over a typical month.

Power Management Savings Potential

This perspective provides an analysis of the energy that might be saved if the power- on profile for the computer system were optimized through active power management technology. Savings potential is calculated from an optimal use standpoint.

System Energy Profile

This perspective depicts an energy profile for each computer system in the visualized environment. For each system, the observed on-time is compared with the optimized-on time achievable with a power management solution. The potential for additional energy savings is also quantified.

Energy Cost Detail

This perspective details energy costs for each computer system. Direct electricity costs, indirect cooling costs, and the total operation cost are provided with average consumption in watts during power-on periods and the typical percentage of time that the computer system in powered on.

Candidates for Power Management

Systems found in the lower right may be good candidates for a power management solution. Systems in the upper left quadrant are exhibiting unpredictable behavior and have little to gain from power management software.

Electricity Waste

Desktops in the upper right are extremely wasteful on electricity use, which can be recovered by implementing a power management solution.

4.2.2.12. Software Packages

Provides insight into the behavior and use of software packages, which are collections of applications.

The Software Packages dataset provides the following perspectives:

Basic

This perspective delivers a high-level view of the software packages used. For each software package, key metrics that indicate the typical, overall resource consumption of the software package along with usage data that helps qualify how it is used are shown.

CPU Technical Analysis

This perspective provides deeper technical data regarding CPU consumption by each software package. Statistical data offered here promotes a finer level of understanding of the processor resource utilization for each software package.

Memory Technical Analysis

This perspective provides deeper technical data regarding memory consumption by each software package. Statistical data offered here promotes a finer level of understanding of the memory resource requirements for each software package.

I/O Technical Analysis

This perspective provides deeper technical data regarding disk I/O consumption by each software package. Statistical data offered here promotes a finer level of understanding of the I/O behavior of each software package.

Usage Summary

This perspective further qualifies how software packages are used. More detailed data regarding usage patterns may be helpful in planning support for these software packages.

Package Workload Details

Data delivered in this perspective helps to size the overall workload presented by a software package as operated by the group of systems. Detailed technical data shown here clarifies how a particular software package presents a workload for the computing environment on which it runs.

Named User vs. Per Device licensing

This perspective helps the IT architect to select application licensing modes that are most economically efficient for the visualized environment. Available licensing models vary widely by application, but this perspective helps to contrast the use of software packages by named users versus systems on which the application may be installed.

Configuration Details

This perspective provides an analysis of the GPU and video support requirements, the Microsoft .NET framework requirements, and the Microsoft run time libraries that are required by each software package.

Unused Software

This perspective provides an analysis of software packages that are installed on systems but are potentially unused. Different columns reflect the period over which no use has been detected. In most cases, software licensing and maintenance costs can be reduced by minimizing the amount of unused software.

Usage Detail

This perspective provides details of usage patterns for software packages. Different columns reflect the number of systems on which the software was installed, the number of systems on which the software package was used, the number of user accounts that used the software package, the estimated accuracy of the usage data displayed, and the number of systems by period over which no use has been detected.

Systems Installed vs. Used

This perspective shows how the number of systems installed compares with the number of users of the system for each software package.

Usage Data Accuracy

This perspective shows how the accuracy of the software usage detection algorithm varies with the number of installed systems for each software package.

Unused Software: 30 Days

This perspective shows how the number of instances of the software package that have been unused for the past 30 days compares with the total number of installations of the software package.

Unused Software: 60 Days

This perspective shows how the number of instances of the software package that have been unused for the past 60 days compares with the total number of installations of the software package.

Unused Software: 90 Days

This perspective shows how the number of instances of the software package that have been unused for the past 90 days compares with the total number of installations of the software package.

Software Package CPU/MEM Usage

Software packages that consume the most resources when in use have the greatest impact to the IT infrastructure overall especially when virtualized. These applications require the greatest amount of CPU and memory resources.

Software Package Disk/SAN Usage

Software packages that produce the most data can be found on the far right of this graph. Those near the top are those that consume the most data. Software packages found in the upper left are those that may benefit the most from SAN implementation for the data storage. These packages benefit greatly from IO read cached appliances because the applications are most likely to be reading similar data across the enterprise.

4.2.2.13. Storage

Describes the amount of storage that is in use on each computer system and how that storage is used.

The Storage dataset provides the following perspectives:

Basic

This perspective shows the most important aspects of disk storage in use on systems.

Storage Full Details

This perspective shows full details of disk storage in use on systems.

Storage with High Redundancy Potential

This perspective shows storage usage on computer systems for which desktop image sharing through virtualization and pooling and/or disk storage de-duplication is likely to have the greatest benefit.

Potential for Slow Login Due to Large Profiles

This perspective shows computer systems where the size of user profiles is larger than optimal for fast login times. Large user profiles may slow logins due to the amount of information transferred during the login process; such profiles should be optimized to improve user experience.

Systems by Total Storage Consumed

This perspective shows systems according to total storage space consumed and user file space consumption.

4.2.2.14. System Mobility

Provides insight into the behavior and mobility needs of the systems. Information in this dataset provides details on how systems in the organization move between subnets and provides an understanding of the mobility needs of the organization.

Each collection in the organization is presented in this dataset to provide information about how that collection compares to the mobility of other organizational collections and the special mobility needs of the various collections in the organization.

The System Mobility dataset provides the following perspectives:

Basic

This perspective identifies the general attributes of computer mobility across the enterprise for all collections.

Subnet Usage Detail

This perspective identifies the overall attributes of computer mobility across the enterprise for all collections. It provides a way to analyse subnet use for all collections within the enterprise and indicates general subnet usage.

4.2.2.15. Analysis

Displays a system versus system or group versus group data comparison. You can use this tool to gain a better understanding of the system or group is performing versus others, using nearly all the data available with LDI Plus. The columns available for graphing have further detail when you hover over them.

Analyse data using the following tabs:

Systems: System versus system metric graphing comparison

Milestones: Historic event graphing of alarms, events, sensors, and more

Groups: Group versus group metric graphing comparison

Hosts: Server versus server metric graphing comparison

Storage: Disk space graphing

4.2.3 Risk Analysis

The Risk Analysis dashboard module presents data views to assist in identifying areas ofpotential security risk, including details of application configurations and inventory, hardware and system configurations, and installed software packages.

4.2.3.1. Dashboard

Provides an overview of the information available from the Risk Analysis dashboard.

4.2.3.2. Application Security

Provides information about which applications might provide a securityrisk. The Application Security dataset only uses the Basic perspective.

4.2.3.3. Security Risk

Provides an indication of the security risk posed by the system based on avariety of factors, including web browsing exposure and software update status.

The Security Risk dataset provides the following perspectives:

Basic

This perspective offers an overview of systems and related information helpful in ensuring security.

Access Control

This perspective shows the Access Control component of the security risk including expired passwords, virus scanner status, and security events.

Browsing

This perspective shows the internet browser component of the security risk including web browsing exposure, non-standard browsers, and Internet Explorer trusted sites.

Software

This perspective shows the software component of the security risk including newapplications running, privileged applications, and apps with multiple execution paths.

Communications

This perspective shows the communications component of the security risk includingoutbound connections, listening ports, and remote desktop usage.

OS Configuration

This perspective shows the operating system component of the security risk including pending update status, screen lock policy, and non-standard screen savers.

Data

This perspective shows the data component of the security risk including file shares, USB storage, old product files, and old user profiles.

4.2.3.4. Systems with Risky Applications

Shows the counts of applications by systems that might present a security risk. The Systems with Risky Applications dataset only uses the Basic perspective.

4.2.3.5. User Security

Provides information about users, their accounts, and privileges that mayimpact the level of information security available from the visualized environment.

The User Security dataset provides the following perspectives:

Basic

This perspective offers an overview of users and related information thatmay be helpful in ensuring security. Some security configurations also have implications for how applications are delivered to the user community. Information related to the privilege level afforded each user,password change and expiration states, and logon usage data provides a starting point for user security analysis.

Users with Administrator Privileges

This perspective lists details for users who operate with administrativeprivileges enabled. These user accounts should be carefully controlled and monitored to avoid security breaches.

Users with Passwords More than 90 Days Old

This perspective lists details for users who have not changed their password in the past 90 days. Regular password changes help ensure theintegrity of user accounts.

Accounts with no Login During Last 21 Days

This perspective lists user accounts that have not been used to begin anew interactive login session in the past 21 days.

Users with Operator Privileges

This perspective lists users who have been granted print operator,communications operator, server operator, or account operator privileges.

Expired User Accounts

This perspective lists user accounts that have expired.

Accounts with Expired Passwords

This perspective lists user accounts with passwords that have expired.

Accounts that do not Require a Password

This perspective lists user accounts that do not require a password.

Accounts where the Password cannot be Changed

This perspective lists user accounts where the user is not permitted tochange the password.

Accounts whose Password does not Expire

This perspective lists user accounts whose passwords have no expiration date.

Accounts where the Password is Stored with Reversible Encryption in AD

This perspective lists user accounts whose passwords are stored with reversible encryption in the Active Directory.

Sensitive Accounts where Delegation is Prohibited

This perspective lists user accounts that are marked as sensitive. Otherusers cannot act as delegates of such user accounts.

Accounts where Logon with a Smartcard is Required

This perspective lists user accounts where the user is required to log onto the account with a smart card.

Accounts where DES Encryption is Required for Keys

This perspective lists user accounts where the principle is restricted touse only Data Encryption Standard (DES) encryption type for keys.

Accounts that are Trusted for Delegation

This perspective lists user accounts where the account is enabled for delegation. This setting allows a service running under the account to assume a client's identity and to authenticate as that user to other remote servers on the network. Accounts with this option enabled should be tightly controlled.

Password Risk Assessment

This perspective shows user accounts (located in the upper right quadrant) that expose the greatest risk to encapsulation/decryptionhacking attempts (assuming all accounts follow the same password policy).

Accounts with the most authentication challenges and the oldest passwords have transmitted easily cracked security information over thenetwork the greatest number of times.

4.2.3.6. Analysis

Refer to Analysis.

4.2.4 Persona Summary

Personas provide abstract models of real users' systems based on work patterns, behaviors, and tools of actual systems in the environment. The Persona module distils users down to amanageable number of user types defined by workstyle (Deskbound, Non-Deskbound, Shared, Industrial) and roles (Power, Task, Knowledge). Real-time data allows an organization to understand what a persona requires from a hardware, software, mobility,

security, and software perspective to aid in effectively provisioning support resources, including budget and personnel, to maximize the end user experience.

Note: No personal identifiable information is available through these modules. Anyreferences to user or individual user show only a system name for a device.

4.2.4.1. Dashboard

Provides an overview of information relating to Persona Analysis.

4.2.4.2. Persona Critical Applications

Provides insight into the critical applications for personas. Persona Critical applications areapplications which consume on average, greater than 5% of a user's total focus time, and have been used by at least 50% of the users that belong to the persona.

The Critical Applications dataset provides a Basic perspective for the various personas including data both presented in a chart and listed in a grid for the number of critical applications, the number of applications, and the number of users belonging to a persona.

4.2.4.3. User Critical Applications

Provides insight into the critical applications for individual users. User critical applications are applications which consume a large portion of a user's total focus time.

The User Critical Applications dataset provides the following perspectives:

Basic

This perspective provides an overview of the critical applications used by individual users.

By Persona

This perspective provides an overview of the critical applications used by users and grouped by persona.

4.2.4.4. User Details

Provides insight into the behavior and needs of the user community, including statistical data and key performance indicators for each user to assist in understanding resource demands, diversity of systems, applications accessed, and user experience.

The User Details dataset provides the following perspectives:

Basic

This perspective provides a high-level overview of the users that are served by the computer systems. For each user, the login hours per week (including display lock and screen saver time), average resource consumption, count of systems used, and count of software packages used are shown.

CPU Technical Analysis

This perspective provides more detailed technical information about the memory demands presented by each user. This deeper detail may provide further insight into the load presented by each member in the visualized community.

Memory Technical Analysis

This perspective provides more detailed technical information about the memory demands presented by each user. This deeper detail may provide further insight into the load presented by each member in the visualized community.

I/O Technical Analysis

This perspective provides more detailed technical information about the disk I/O demands presented by each user. This deeper detail may provide further insight into the load presented by each member of the visualized community.

I/O Read and Write Technical Details

This perspective shows disk I/O technical information, including separate statistics for read and write activity for each member of the visualized user community. This information is likely to be useful in the design of an efficiently performing storage subsystem by the IT architect.

Usage Summary

This perspective shows more detailed technical information about how each member of the visualized community uses computing resources. The IT architect may find it helpful to understand these workload details when designing the application delivery infrastructure.

Application Startup Experience

This perspective offers insight into the start-up delay experienced by users across all applications that they use. While some applications inherently require more time to start due to others due to processing requirements during the load sequence, statistical measurements offered here may help to depict typical delays across the user community.

Application Workload Details

Data delivered in this perspective helps to size the overall workload presented by a user in the visualized environment across the full software package and application set. Detailed technical data shown here clarifies how a particular user presents for the computing environment used.

Login Configuration

Data offered in this perspective describes the aspects of the environment that support login of users in the visualized environment. Information shown here may be helpful in planning and optimizing login time through careful planning of the events that take place during user login.

Security Attributes

Data offered in this perspective describes the aspects of the environment that relate to account configurations and account passwords.

User Details

Data offered in this perspective describes the aspects of the environment that describe the configuration details of user accounts in the visualized environment.

Users by Applications and Computer Resources

Users that log in to one computer and use a small subset of enterprise applications can be found in the lower left of the chart. Users that log into many systems and use a wide range of applications can be found in the upper right quadrant.

User Resource Footprint

Users that consume the most resources while active have the greatest impact to the IT infrastructure overall (especially when virtualized). These users (found in the upper right) require the greatest amount of CPU and memory resources.

4.2.4.5. User Resource Consumption

Provides an overview of resource consumption for individual users.

The User Resource Consumption dataset provides the following perspectives:

Basic

This perspective provides an overview of the resource consumption for users.

CPU Consumption by Persona

This perspective provides an overview of the CPU consumption for users grouped by their persona.

Memory Consumption by Persona

This perspective provides an overview of the memory consumption for users grouped by their persona.

IO Consumption by Persona

This perspective provides an overview of the IO consumption for users grouped by their persona.

Network Consumption by Persona

This perspective provides an overview of the network consumption for users grouped by their persona.

4.2.4.6. User Systems

Provides information relating to the systems used by individual users.

The User Systems dataset provides the following perspectives:

Basic

This perspective provides an overview of the systems used by individual users.

By Persona

This perspective provides an overview of the systems used by users with users grouped by their persona.

4.2.4.7. Analysis

Refer to Analysis.

4.2.5 Sector Benchmarks

Sector Benchmarks allows LDI Plus customers to compare key performance indicators (KPIs)from their environment to a representative sample of peer data from other organizations. Peer benchmarking is also helpful for assessing whether your IT environment is at a competitive advantage or disadvantage. While internal benchmarking is important for measuring improvements withing your own environment over time, external benchmarkingenables you to assess your success in a broader context. Access to industry averages can help a customer build a better case for increased attention or investments to improve. Organizations can also answer pressing questions like How is everyone else doing?

Your organization must opt in to view Sector Benchmarks data or have been collecting dataon at least five devices for one week after activation. If you have not met these requirements. Contact your Lenovo support specialist to learn more about accessing Sector Benchmarks data.

Dashboard

Provides an overview of Sector Benchmarks datasets.

Application Faults

Provides an assessment of how many application problems may impact users in the sector. Sector benchmark data is uploaded and processed weekly, so the community statistics may not include data for faults that have recently occurred on your systems.

Boot and Login

Provides boot and login performance data experienced by users for each system in the environment, including boot and login time, initialization sequences for systems, and login and post-boot sequences. It compares that data to a larger peer group within the industry.

Computer Performance

Provides insight into how each computer in the visualized environment is used and how much of their available computing resources are effectively used in delivering applicationsto users. It compares that data to a larger peer group within the industry.

Hardware

Provides asset and configuration data that describes the fundamentals of the environment delivered to the user. Data and key descriptive indicators are not included for each hardware system to understand and plan the IT environment.

This perspective identifies software packages that contain one or more Internet Explorer extensions. Such software packages may require special consideration if they are to be delivered through application virtualization.

Storage

Describes the amount of storage in use on each computer system and how it is being used. It helps to identify inappropriate storage configurations or users to minimize storage costs and waste, improving user experience.

4.5.1. Analysis

Refer to Analysis.

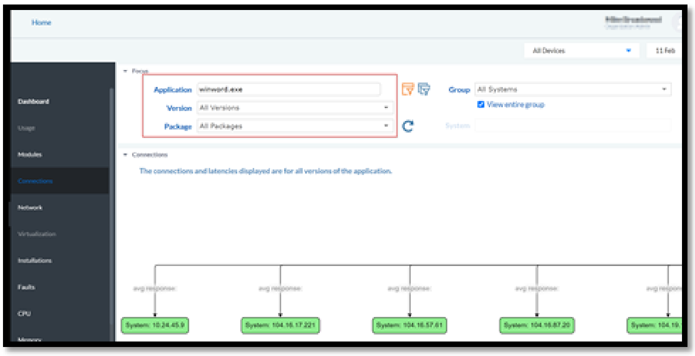
4.3 App Vision

App Vision provides a centralized location for viewing application health. The scope of application health can range from developers interested in the performance or stability of a home-grown enterprise application to monitoring performance of a SaaS app and reporting bugs to the vendor.

App Vision provides real-time application performance data that can be filtered by application, package, or version. It is updated every ten minutes and provides the ability to see data at the organization or grouped system level, as well as the individual system level.

Using App Vision

1. Select **App Vision → Modules**. You can also double click an application listed in the **Dashboard**.
2. Type any part of an application name in the **Application** field to narrow down the options,

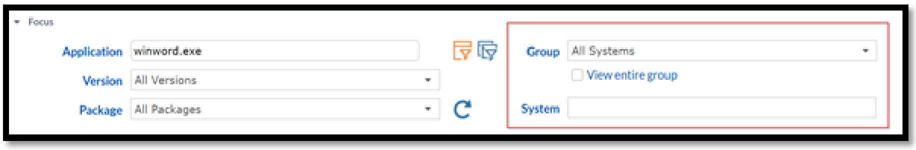


Application winword.exe
Version All Versions
Package All Packages
Group All Systems
☑ View entire group
System

The connections and latencies displayed are for all versions of the application.

then select one from the list. You can also choose a specific version and package.

To see data for a **specific system** within a group, de-select the **View entire group** option, and then select a specific system.



Focus

Application: winword.exe

Version: All Versions

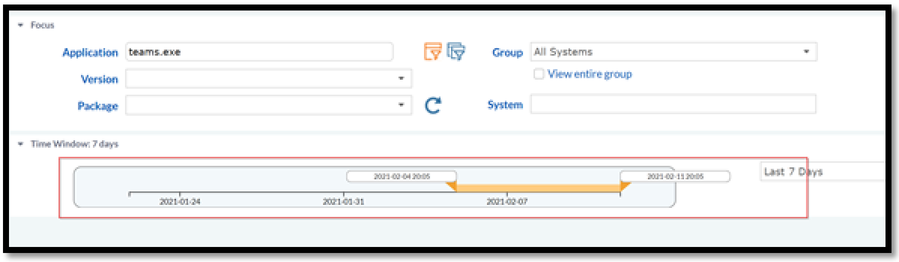
Package: All Packages

Group: All Systems

□ View entire group

System:

Start and end times can also be adjusted, as well as a different time range. When looking at a group of systems, the local time for the systems running App Vision is used. When looking at a specific system, the target system’s local time is used.



Focus

Application: teams.exe

Version:

Package:

Group: All Systems

□ View entire group

System:

Time Window: 7 days

2021-02-04 20:05 – 2021-02-11 20:05

Last 7 Days

By default, App Vision filters by application. To select a package, filter by **Package** option. Then, select a package, specific application, and version. You can click the **Reload** ↻ icon to get results. Each time changes are made to the header area, click the **Reload** ↻ icon get the relevant data.

4.3.1 Dashboard

Provides information about the applications, their usage, and the resources consumed.

4.3.2 Modules

Displays the modules that the selected application calls. The page also displays the runtimes that are currently running to support the selected application. The time window is not available on this page, as it returns current information.

4.3.3 Connections

Shows what other systems the selected application is currently connected to and the average response time. The connection and latencies are shown for all versions of the selected application. If the target system is in LDI Plus, the page shows that system’s location. The connections section is based on application latency over the last 90 days. The App Vision data is aggregated from systems across the environment. This uses server-level data, so the systems aren’t required to be online at the time.

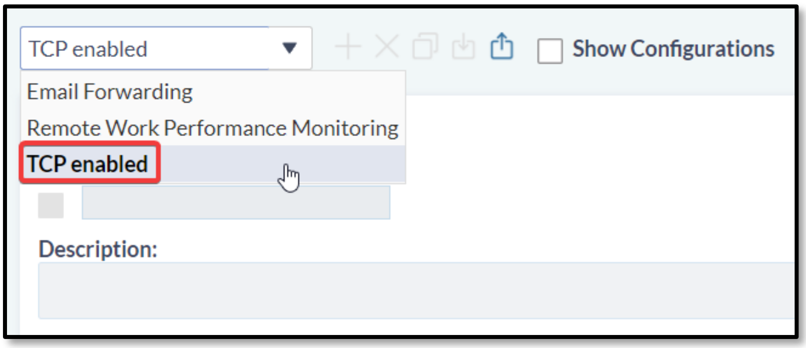
4.3.4 Network Graphing

Shows data about network I/O for the selected application. It also shows the total number of connections and peak number connections during the selected time window.

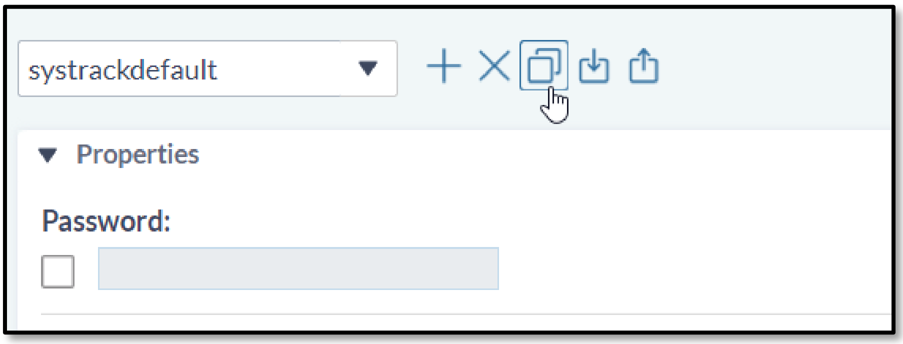
If TCP connection is not enabled, you need to enable it. This view helps you to perform live queries with the various agents, but it also increases the size of the database significantly. The servers can handle that but reporting and queries might slow down a bit depending on what you are looking for because the cloud is now sifting through the extra data. This is a great setting if you are looking for an application causing issues in real time, but not very efficient if you are just running an inventory of installed apps on the agent.

To enable TCP connection:

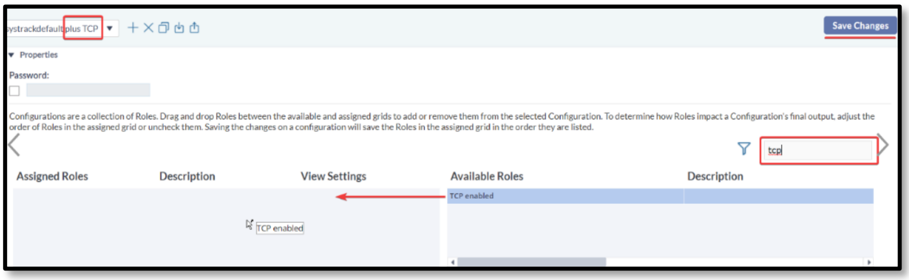
1. Select Configuration → Insights & Automations → Role Management.
2. Click the 🔒 lock icon in the top right of the page.
3. Click the roles drop-down and check if there is already a role for your organization that includes TCP enabled. if not, select **Plus** + icon to create a new role and name it accordingly for TCP Enabling.



4. In the **Views** tab, select the **TCP Connections** option.
5. Click **Save Changes** in the top right of the page.
6. In the **Policies** sub menu ensuring the lock is still unlocked, make sure the Policy drop-down systrackdefault is enabled.
7. Click the duplicate rectangles icon to duplicate this Policy so that all the same rules and configurations that you have been using are used and name the duplicate accordingly.



8. Search for your new TCP enabled Role you previously made in the search bar and drag it from the rightmost **Available Roles** to the leftmost **Assigned Roles** column and click **Save Changes** in the top right.


Configurations are a collection of Roles. Drag and drop Roles between the available and assigned grids to add or remove them from the selected Configuration. To determine how Roles impact a Configuration's final output, adjust the order of Roles in the assigned grid or uncheck them. Saving the changes on a configuration will save the Roles in the assigned grid in the order they are listed.

9. In the **System Assignments** sub menu, change the Configuration drop-down option for each device you want to use the TCP enabled policy.

10. In the Administration sub menu, select systrackdefault in the Set default configuration for new systems: drop-down list.
11. In the **Administration** sub menu, select each device and then select the **Read Configuration & Run** button to ensure that the change is made immediately.
12. You see an updated status of the configuration in the table below the **Run** button. Congratulations! You've just learnt how to set up a new Configuration Policy and enabled TCP analytics for the devices you selected in your organization!

4.3.5 Virtualization

Provides information about the virtualization complexity of the software package. Click on a cell in the Drill down Available grid to bring up additional detail. If you choose an application version, the virtualization tab becomes clickable. This gives the application version a complexity score if you were to move it from a physical device to a virtual one. The complexity score looks at different dependencies that are required for the device, as well as its supportability by different OS.

4.3.6 Installations

Provides information about the selected application such as the version and date it was installed. If a specific software package is selected instead of All Packages, the grid shows more information, such as the systems on which the package is installed and the last used date.

4.3.7 Faults

4.3.8 CPU

Displays the faults that have occurred on the selected application. These can be hard or soft faults depending on the application, but often they are impacting user experience with the application. This would be information to take to an application owner or to a vendor. Most often, this would be updating a particular version of an application where the vendor has remedied the issue but sometimes the vendor canbe unaware, and this provides very useful data so they can make the fix. Provides information about CPU utilization, including overall utilization and usage while active.

4.3.9 Memory

Displays memory-related data like peak usage and page faults per second.

4.3.10 I/O

Displays information pertaining to Read and Write I/O.

4.3.11 Network

Provides network usage data for the application, including the average number of packets received and transmitted for all systems and for specific systems.

Times- Displays information on load time and active time.

GPU- Provides information about the GPU used, if any.

4.3.12 Systems

Displays information about the systems the selected application is run on and the number of users. Clicking the number of an item displays additional detail information.

4.4 Device Lookup

4.4.1 Overview

Built for use by Service or Help Desk personnel, Device Lookup provides heightened visibility into physical and virtual user desktops to enable IT quickly diagnose problems, enhancing end user experience and productivity while reducing IT personnel involvement. Device Lookup empowers technicians to diagnose user service issues using powerful features to analyse between the problem system and all physical and virtual user systems or any subset to identify and learn where behavior diverges from the normal ones.

Device Lookup reduces the amount of time each service technician spends per call, reduces the number of call escalations, and increases the call resolution ratio. Device Lookup continuously monitors literally hundreds of performance objects on every user system in the environment – tracking application behavior, system performance, and changes to the user system configuration. Alerted as specified thresholds are exceeded, technicians can make the necessary adjustments to proactively correct the problem.

Major Features

- Automated diagnostics
- Deep visibility and insight into physical and virtual desktops from a single console
- Proactive identification of nascent problems through continuous real-time monitoring
- Built on massively scalable, distributed relational database technology for data collection, aggregation, and presentation

Key Benefits

- Improved IT efficiency and cost savings through reduced problem time-to- resolution
- Improved quality of service (QoS) delivery through enhanced user productivity and satisfaction
- Reduces Help Desk service calls

How Device Lookup Works

Device Lookup helps you to prioritize issues and then taking actions for immediate remediation. Identification of larger trends in the environment through Fleet View leads to conclusive ranking of systems and triage, which enables granular analysis in Device Lookup.

Device Lookup completes the overall portrait of enterprise system performance by filling in the necessary low-level details required to make definitive recommendations. By coupling this system-level analysis to overall trending information, the impact of decisions can be seen clearly, completing the information loop, and enabling easy environmental optimization. Device Lookup allows continual improvement to end-user productivity and satisfaction by simplifying and automating the problem-solving process while still allowing deep insight into the evolution of emerging trends.

Device Lookup presents a detailed analysis of each system's history of usage. Multiple views of critical system information can be viewed over selected periods of time. Examples of these detailed views for individual systems include:

- Generated alarms, along with an explanation of the alarms and in most cases a recommendation for improvement.
- Applications view provides point-in-time per-process visibility for a system including Process ID and all associated performance utilization metrics.
- A detailed history of CPU, memory, storage, and IOPS usage.
- A health score that is easily compared to trending data from Fleet View, which maintains up to three years of history.
- A system dependency map that includes a history of systems used to access the targeted system, mapped drives, application dependencies, and network latencies to and from dependent and back-end servers.
- Boot times and system login processes mapped and displayed to assist in problem determination.
- Interactive ad-hoc graphs for selected system metrics and milestones over a specified time range. Multiple graphs are overlaid, allowing you to easily view and compare related concerns.
- A complete history of application usage. This includes when applications have been added and/or modified.
- For support personnel with proper authorization, a rollback option is available to reset the system's OS to a previous level if/when required.

Focus System

Selecting the Focus System

Device Lookup is a help desk utility that helps you identify issues with a particular system. Before you can begin using the Device Lookup analytics tools to identify issues, you need to first select the system you want to focus on.

To select the focus system:

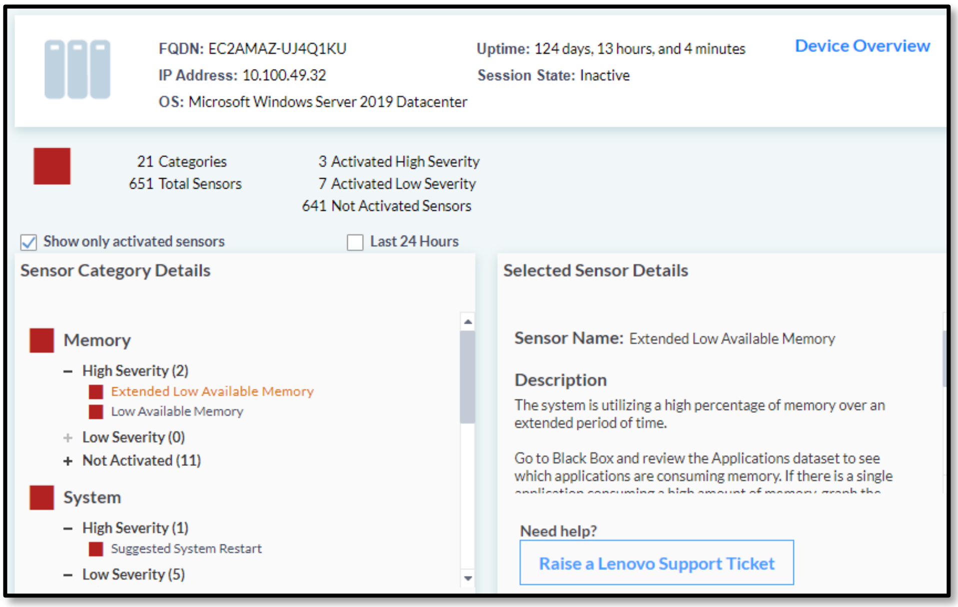
1. If your environment has many systems, you may want to first apply a **Groupfilter** to narrow down the searchable systems.

To apply a group filter:

   a. Select the group's name from the **Filter by Group** drop-down. As you enter text, the choices in the drop-down menu are filtered to match the entered text.
   b. Click to select the group from the resulting list.

2. To search for and select a system:
   a. Enter all or part of a system's name or IP address in the **Find System** field. The systems associated with the entered system or IP address appear.The **Chassis** field provides the type of system.
   b. Click to select the focus system.
3. Device Lookup is now connected directly to the selected system. After Device Lookup executes a diagnostic routine on the system the Overview Diagnostics screenopens, displaying the system's diagnostics results.

Information identifying the system selected as the focus (and the system's time) displays on Device Lookup's title bar.



FQDN: EC2AMAZ-UJ4Q1KU
IP Address: 10.100.49.32
OS: Microsoft Windows Server 2019 Datacenter

Uptime: 124 days, 13 hours, and 4 minutes
Session State: Inactive

Device Overview

🟥 21 Categories
651 Total Sensors

3 Activated High Severity
7 Activated Low Severity
641 Not Activated Sensors

☑ Show only activated sensors
□ Last 24 Hours

Sensor Category Details

🟥 Memory
– High Severity (2)
🟥 Extended Low Available Memory
🟥 Low Available Memory
+ Low Severity (0)
+ Not Activated (11)

🟥 System
– High Severity (1)
🟥 Suggested System Restart
– Low Severity (5)

Selected Sensor Details

Sensor Name: Extended Low Available Memory

Description

The system is utilizing a high percentage of memory over an extended period of time.

Go to Black Box and review the Applications dataset to see which applications are consuming memory. If there is a single application consuming a high amount of memory, graph the

Need help?

Raise a Lenovo Support Ticket

Once connected to a focus system, Device Lookup executes a system diagnostic routine. The Overview page opens displaying the results of the system diagnostics. In some cases, further analysis is required, and other Device Lookup tools can be utilized to quickly identify the root cause of the problem, providing the information needed to Device Lookup.

The Overview page provides basic system information such as the Device Details, Warranty Details, Health Trend Analysis, Critical Sensors, etc. The bottom pane of the screen, the Applications Fault Details provides quick insight into system issues.

Using the Deployment Tool, a set of categorized rules are configured and applied to systems. After deployment, the set of rules are run in the background on the system. The Overview Diagnostics pane displays the color-coded rule states (as defined below) for the rules within each rule category.

- Green: rule passed
- Yellow: warning state
- Red: critical state

The rule category itself has a color-coded diagnostic state. The criteria for determining the rule category state are as follows:

- If any of the rules within the category have a critical state, the rule category also have a critical state.
- If no rules within the category have a critical state, and one rule has a warning state, the rule category has a warning state.
- If no rules within the category have a critical state, and more than one rule has a warning state, the rule category has a critical state.
- If all rules in the category pass, the rule category also passes.

The criterion for determining the overall diagnostic state is as described above but are applied at the category level instead of rule level. For example, if one category has a warning state, the overall diagnostic level has a warning state, but if more than one category has a warning state, the overall diagnostic level has a critical state.

When you hover over a rule category in the Diagnostic Category Details pane, a description of the category displays. When you click a rule, a description of the rule and a recommended action display in the right detail pane.

By default, show only critical and warnings is enabled. When enabled, only the categories that have critical and warning states display (along with any tests that pass within the categories). Disable this option to display rule results.

Basic Tool Descriptions

The following table describes each tool found in Device Lookup.

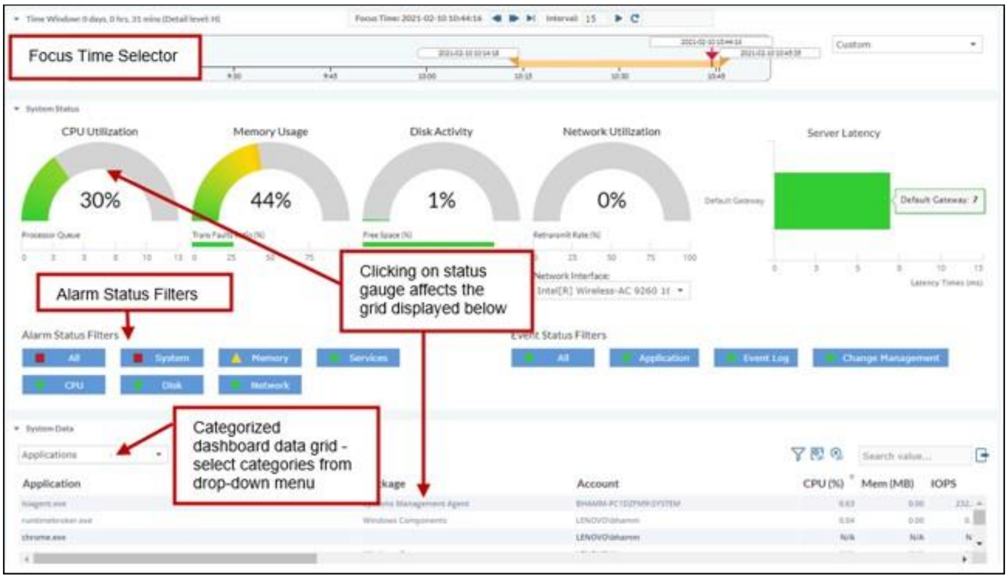
Basic Tool	Description
Dashboard	Provides a quick system overview, allowing you to easily determine if there are issues that need further investigation.
BlackBox	Works similarly to the Dashboard Tool, with the addition of a graph that allows you to rewind to a point in time and review detailed system data (e.g., alarms and applications that were active at that time).
Health	Provides a look at the system's health score (the service quality) over the past thirty days.
System Usage	Provides a graphical summary of the system's utilization over the last thirty days.
Dependencies	Provides a system dependency map that includes a history of systems used toaccess the targeted system, local and mapped drives, application dependencies, and network latencies to and from dependent databases and servers.
Hardware	Provides an inventory of the system's hardware.
Hardware Diagram	Provides a mapping of all the peripherals connected to or part of a selected device.
Software	Provides a history of software package changes, installations, and usage for the selected time.
Faults	Identifies the software package faults that have impacted the system during the selected time.

4.4.2 Dashboard

Through Master Alarms and categories of system data, the dashboard allows you to quickly identify possible problem areas for a specific point in time. Once a potential problem area has been identified and related Dashboard data reviewed, you can then use other Device Lookup tools, such as Black Box, to dive deeper into the details.

The Dashboard is composed of the following:

- Alarm Status Filters
- Focus Time Selector
- Categorized System Status Dashboard and System Status Data Grid



Dashboard Alarm Status Filters

The Alarm Status Filters in the System Status panel on the Device Lookup Dashboard provide a color-coded graphical overview of issues affecting the system corresponding to the date range selected on the focus date/time bar.

When you click the **Alarm Status Filter** button, it displays the active alarms for that alarm category.

Click the **All** button to display the active alarms for all classifications. The color-coding for the Alarm Status Filter buttons is as follows:

- Red: The classification has at least one active alarm with a critical security level.
- Yellow: The classification has at least one active alarm with a warning security level.
- Green: The classification has no active alarms (if you select a green button, no data displays)

Many of the Filter entries are normal changes that were detected.

The following table provides the data category that is displayed for each of the related data dashboard items.

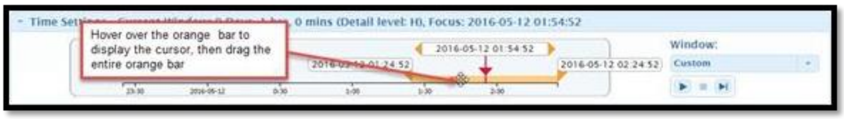
Dashboard Button	Resulting Data Category
CPU Utilization	Applications, sorted by CPU
Memory Usage	Applications, sorted by MEM
Disk Activity	Applications, sorted by IOPS
Network Utilization	Connections

Adjust the Focus Time

The current date/time displayed reflects the focus time for the tool's data – allow you to use the system status display (data grid) to review what was happening on the system at the specific point in time as well as change the date and time range.

If you change the focus time in the Dashboard it is also changed in the Black Box.

Use the following methods to change the focus time:



Time Settings - Current Window: 0 Days, 1 hrs, 0 mins (Detail level: H), Focus: 2016-05-12 01:54:52

Hover over the orange bar to display the cursor, then drag the entire orange bar

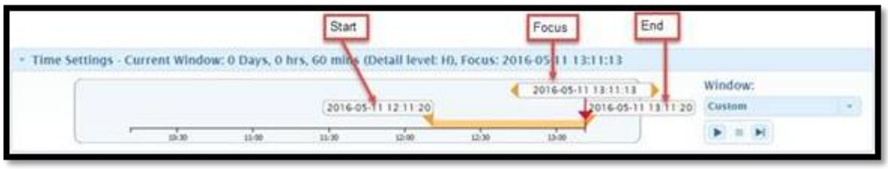
2016-05-12 01:24:52

2016-05-12 01:54:52

2016-05-12 02:24:52

Window: Custom

2. Drag the entire orange bar
3. Pull and drag either end of the orange bar to change the end or startdate/time
4. Drag the bottom of the red arrow to change to current focus time (availableon the System Dashboard and Black Box)
5. Manually change the start, focus, or end date/time by placing your cursor in one of the three date/time fields to display a blue highlight. Enter the desired focus time. When completed, click outside the field for the change to take effect.



Start

Focus

End

Time Settings - Current Window: 0 Days, 0 hrs, 60 mins (Detail level: H), Focus: 2016-05-11 13:11:13

2016-05-11 12:11:20

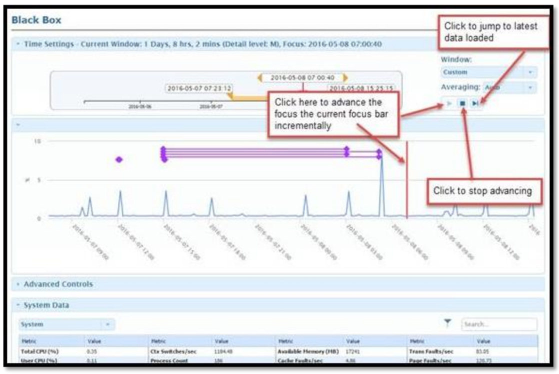
2016-05-11 13:11:13

2016-05-11 13:11:20

Window: Custom

Select a time frame from the **Window** drop-down field (default value is Custom)

Use the load function buttons to advance the current focus incrementally.



Black Box

Time Settings - Current Window: 1 Days, 8 hrs, 2 mins (Detail level: M), Focus: 2016-05-08 07:00:40

Click to jump to latest data loaded

Window: Custom

Averaging: Auto

Click here to advance the focus the current focus bar incrementally

Click to stop advancing

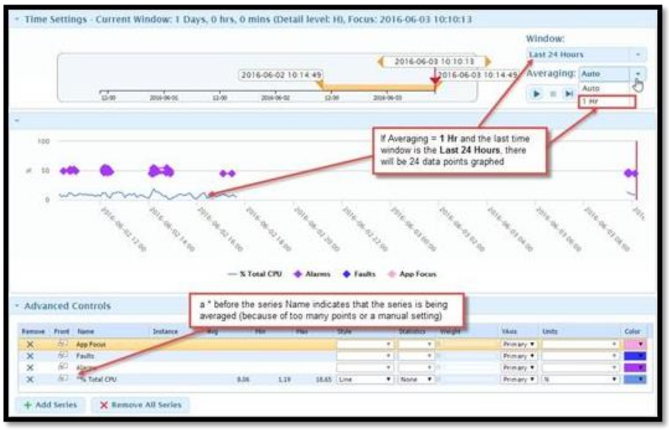
Advanced Controls

System Data

Select the Averaging Function

The **Averaging** setting controls how the raw data points are treated before being graphed. If **Auto** is selected, the raw data points are graphed without being altered if there are not too many points to graph (high detail and/or long window time). The maximum number of points that can be graphed is 500. Above that, the chart averages the points so that they meet the 500-point maximum. If the setting is anything other than Auto, the data is averaged into periods as defined by the setting. For example, if the Averaging setting is 1 hour and the time window is the last 24 hours, there are 24 data points graphed. If the raw data is at a higher sample rate than 1 hour, the points occurring ineach hour are averaged to get the value for that hour's data point.

When a series is being averaged (because of too many points or a manual setting), a * proceeds the series name.



Time Settings - Current Window: 1 Days, 0 hrs, 0 mins (Detail level: H), Focus: 2016-06-03 10:10:13

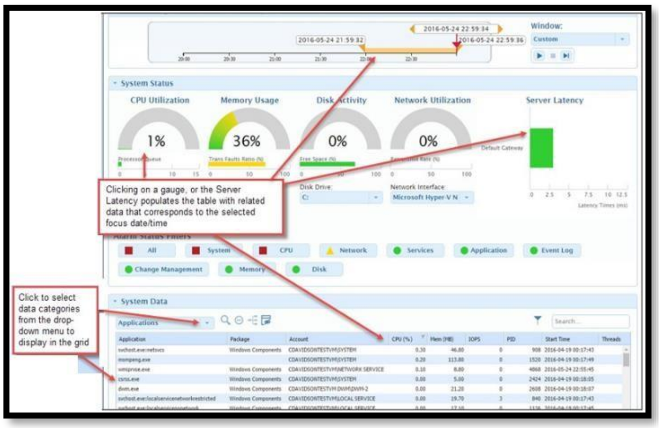
Window: Last 24 Hours

Averaging: Auto

If Averaging = **1 Hr** and the last time window is the **Last 24 Hours**, there will be 24 data points graphed

a * before the series Name indicates that the series is being averaged (because of too many points or a manual setting)

Dashboard System Data Grid



Clicking on a gauge, or the Server Latency populates the table with related data that corresponds to the selected focus date/time

Click to select data categories from the drop-down menu to display in the grid

Window: Custom

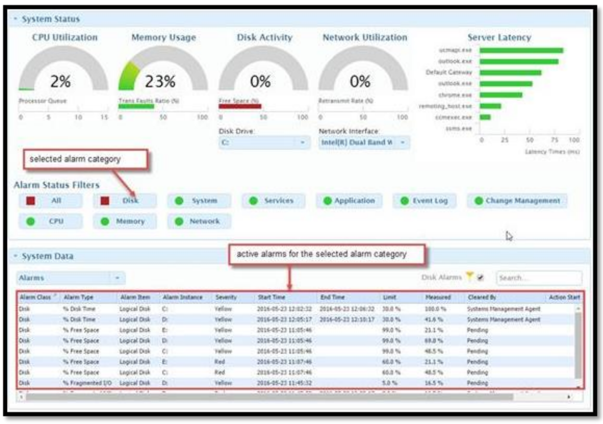
When you select an item from the System Status, related data displays in the dashboard data grid. For each selection, whether it's from the Alarm Dashboard or one of the data grids tabs, the data displayed corresponds with the selected Focus Time.

The following items provide a detailed description of the data displayed when you select the data categories from the drop-down menu located at the top of the System Datagrid:

Alarms

When you select an alarm category button from the Alarm Dashboard, the table displays data for the category's alarms that were active at the Focus Time. Active alarms arethose with critical (red) or warning (yellow) severity levels.

When you select the Alarms category, data for the last alarm category button selected displays. The screenshot below calls out an example grouping, with the Disk Alarm Filter Status button selected. The screenshot also shows the details displayed when you hover over oneof the meter readings.



selected alarm category

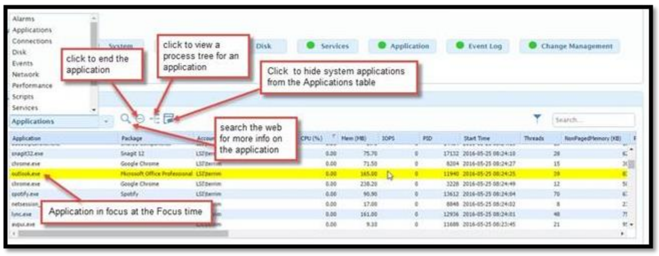
active alarms for the selected alarm category

Alarm Class	Alarm Type	Alarm Item	Alarm Instance	Severity	Start Time	End Time	Limit	Measured	Cleared By	Action Start
Disk	% Disk Time	Logical Disk	C:	Yellow	2016-05-23 12:02:32	2016-05-23 12:06:32	30.0 %	100.0 %	Systems Management Agent	
Disk	% Disk Time	Logical Disk	D:	Yellow	2016-05-23 12:05:17	2016-05-23 12:10:17	30.0 %	41.6 %	Systems Management Agent	
Disk	% Free Space	Logical Disk	E:	Yellow	2016-05-23 11:05:46		99.0 %	21.1 %	Pending	
Disk	% Free Space	Logical Disk	D:	Yellow	2016-05-23 11:05:46		99.0 %	69.8 %	Pending	
Disk	% Free Space	Logical Disk	C:	Yellow	2016-05-23 11:05:46		99.0 %	48.5 %	Pending	
Disk	% Free Space	Logical Disk	E:	Red	2016-05-23 11:07:46		60.0 %	21.1 %	Pending	
Disk	% Free Space	Logical Disk	C:	Red	2016-05-23 11:07:46		60.0 %	48.5 %	Pending	
Disk	% Fragmented I/O	Logical Disk	D:	Yellow	2016-05-23 11:45:32		5.0 %	16.5 %	Pending	

Applications

Selecting this category from the System Data grid menu displays the list of the applications running in the environment at the Focus Time. The highlighted application is the application in focus at that time.

One key use of application data is determining which applications are consuming the most resources. For example, you can sort by CPU to determine which applications are occupying the most CPU. First select an Application from the grid, and then use the icons to the right of the pop-up menu:



click to end the application

click to view a process tree for an application

Click to hide system applications from the Applications table

search the web for more info on the application

Application in focus at the Focus time

Application	Package	Account	CPU (%)	Mem (MB)	IOPS	PID	Start Time	Threads
snagit32.exe	Snagit 12	LS7[illegible]	0.00	75.70	0	17132	2016-05-25 08:24:10	28
chrome.exe	Google Chrome	LS7[illegible]	0.00	71.50	0	8204	2016-05-25 08:24:27	15
outlook.exe	Microsoft Office Professional	LS7\jerrim	0.00	165.00	0	11940	2016-05-25 08:24:25	29
chrome.exe	Google Chrome	LS7\jerrim	0.00	238.20	0	3228	2016-05-25 08:24:49	12
spotify.exe	Spotify	LS7\jerrim	0.00	90.90	0	13612	2016-05-25 08:24:04	70
netsession[illegible]			0.00	17.00	0	8848	2016-05-25 08:24:02	8
lync.exe			0.00	161.00	0	12936	2016-05-25 08:24:01	48
avpui.exe			0.00	9.10	0	11688	2016-05-25 08:23:45	21

Use the search icon to open search results for the Application in your default browser

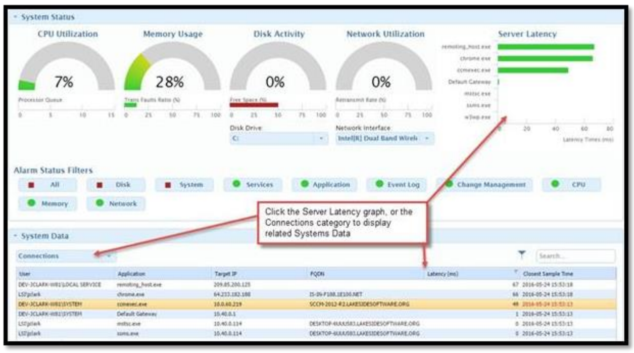
End the Application if you have administrative privileges for the focus system. If the application was running at the Focus Time but is not currently running, this action have no effect.

Hide the system applications from the grid.

View a process tree for the application.

Connections

Clicking on the Server Latency graph in the System Status panel displays this category of data in the System Data grid.



Click the Server Latency graph, or the Connections category to display related Systems Data

User	Application	Target IP	FQDN	Latency (ms)	Closest Sample Time
DEV-JCLARK-W81\LOCAL SERVICE	remoting_host.exe	209.85.200.125		67	2016-05-24 15:53:18
LS7\jclark	chrome.exe	64.233.182.188	IS-IN-F188.1E100.NET	66	2016-05-24 15:53:18
DEV-JCLARK-W81\SYSTEM	ccmexec.exe	10.0.60.219	SCCM-2012-R2.LAKESIDESOFTWARE.ORG	48	2016-05-24 15:53:13
DEV-JCLARK-W81\SYSTEM	Default Gateway	10.40.0.1		1	2016-05-24 15:53:13
LS7\jclark	mstsc.exe	10.40.0.114	DESKTOP-6UUUS83.LAKESIDESOFTWARE.ORG	0	2016-05-24 15:53:13
LS7\jclark	ssms.exe	10.40.0.114	DESKTOP-6UUUS83.LAKESIDESOFTWARE.ORG	0	2016-05-24 15:53:13

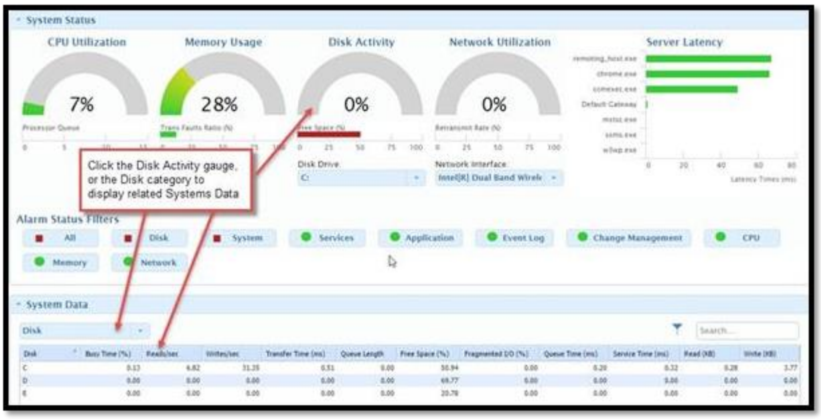
Selecting this category displays data (that corresponds to the Focus Time) for the system's session and remote server dependencies. If there are no dependencies for the Focus Time, no data is displayed.

Session Latency is a measure of the time it takes network traffic packets to get from the user’s interface (e.g., a dumb terminal) to the host of the user’s system and back. Dependency Server Latency is a measure of time it takes network traffic packets to get fromthe system running the application (such as Outlook) to get to and from the server the application is dependent on (such as an Outlook Exchange Server).

If there is a dependency with a relatively high latency time, use the **Dependencies Tool** to investigate further.

Disk

Selecting this category displays an overview of the system's physical drives that correspondsto the Focus Time. Keep in mind that these metrics should be considered in context. For example, if a Disk has a relatively high Disk Time, but the Q Length and Q Time are at an acceptably low level, most probably there is not a performance issue. But, if there is a high Disk Time and a higher-than-normal Q Length, this could indicate that transactions are not being processed in a timely manner.



Click the Disk Activity gauge, or the Disk category to display related Systems Data

Disk	Busy Time (%)	Reads/sec	Writes/sec	Transfer Time (ms)	Queue Length	Free Space (%)	Fragmented I/O (%)	Queue Time (ms)	Service Time (ms)	Read (KB)	Write (KB)
C	0.13	4.82	31.25	0.51	0.00	50.94	0.00	0.20	0.32	0.28	3.77
D	0.00	0.00	0.00	0.00	0.00	69.77	0.00	0.00	0.00	0.00	0.00
E	0.00	0.00	0.00	0.00	0.00	20.78	0.00	0.00	0.00	0.00	0.00

Events

Selecting this category displays event data corresponding to the Focus Time. If a user is not logged into the system, this table has no data.

GPU

Provides information about the focus system's GPU.

Network

Selecting this category displays data (that corresponds to the Focus Time) for the system'snetwork adapter(s).

Reviewing the Broadcast/sec and Retransmit (%) rates give you a sense of utilization on the network interface. If there is an issue, you need to investigate further to determine, for example, if the issue is with the adapter or if there is an external issue.

If the focus system is a virtual machine, you see data for the virtual adapter that provides network connectivity. If the focus system is not a virtualized machine, you see data for the physical adapter.

Performance

Performance is a custom data category. The collection items that display are manually specified for the system.

Power

This category is only included for focus systems that are physical desktops. Selecting this category provides power demand data for the focus system. Although this data may not be meaningful when you are considering just one system, consider the effect of aggregating the cost of the power demand for many systems.

Scripts

This category is only included if a system has a custom script configured via the DeploymentTool. Selecting this category displays data relating to the custom script.

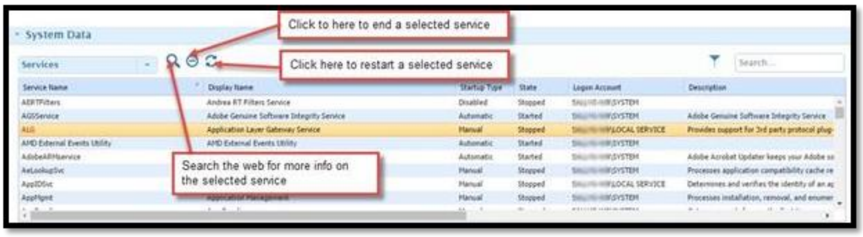
Services

Selecting this category displays Windows Service Control Manager data for the Focus Time. You can use this table to quickly answer questions such as:

What role does the service play (**Description**)?

Does the service start automatically or manually (**Startup Type**)?

Was the service running at the focus time (**State**)?



Click to here to end a selected service

Click here to restart a selected service

Search the web for more info on the selected service

Service Name	Display Name	Startup Type	State	Logon Account	Description
AERTFilters	Andrea RT Filters Service	Disabled	Stopped	[redacted]\SYSTEM	
AGSService	Adobe Genuine Software Integrity Service	Automatic	Started	[redacted]\SYSTEM	Adobe Genuine Software Integrity Service
ALG	Application Layer Gateway Service	Manual	Stopped	[redacted]\LOCAL SERVICE	Provides support for 3rd party protocol plug-
AMD External Events Utility	AMD External Events Utility	Automatic	Started	[redacted]\SYSTEM	
AdobeARMservice		Automatic	Started	[redacted]\SYSTEM	Adobe Acrobat Updater keeps your Adobe so
AeLookupSvc		Manual	Stopped	[redacted]\SYSTEM	Processes application compatibility cache re
AppIDSvc		Manual	Stopped	[redacted]\LOCAL SERVICE	Determines and verifies the identity of an ap
AppMgmt	Application Management	Manual	Stopped	[redacted]\SYSTEM	Processes installation, removal, and enumer

Where was the service running (**Logon Account**)?

Select a Service Name from the grid, and then use the icons to the right of the pop-up menu:

- Use the search icon to open search results for the service in your default browser
- End the service if you have administrative privileges for the focus system
- Restart the service if you have administrative privileges for the focus system

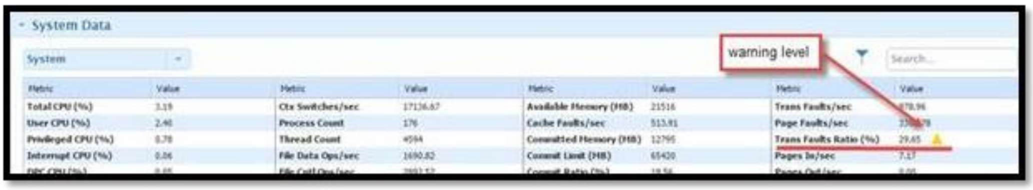
Note: If the State of the Service (Started or Stopped) at the Focus Time is not the current state of the service, these actions have no effect.

Sessions

Selecting this category displays user session data that corresponds to the Focus Time. If a user is not somehow logged in to the system, this table has no data. Key information provided is who is logging in to the system and how they are connecting (using a Console or an RDP connection).

System

Selecting this category provides general system characteristics as numerical values that correspond to the Focus Time. Values marked with red indicate a critical level for the metric.Values marked with yellow indicate a warning level. If a value is not in the expected range, use other Device Lookup tools to investigate further.



Metric	Value	Metric	Value	Metric	Value	Metric	Value
Total CPU (%)	3.19	Ctx Switches/sec	17136.67	Available Memory (MB)	21516	Trans Faults/sec	878.96
User CPU (%)	2.40	Process Count	176	Cache Faults/sec	513.81	Page Faults/sec	[illegible]
Privileged CPU (%)	0.78	Thread Count	4594	Committed Memory (MB)	12795	Trans Faults Ratio (%)	29.65 ⚠
Interrupt CPU (%)	0.06	File Data Ops/sec	1690.82	Commit Limit (MB)	65420	Pages In/sec	7.17
DPC CPU (%)	0.05	File Cntl Ops/sec	2897.12	Commit Ratio (%)	19.56	Pages Out/sec	0.00

To investigate further, you could for example:

- Using the Graphing Tool, add a System Trans Faults/sec series to the graph.
- Using the resulting Trans Faults/sec graph line, click the data point that represents the critical level value.
- Using the resulting Black Box Tool, review what was happening on the system at that point in time.

Virtual Machine

This category is only included for focus systems that are virtual machines. Selecting this category displays information (that corresponds to the Focus Time) about the virtual systemhost and the virtual system memory.

The Virtual System Host data tells you to which host the virtual machine belongs.

The Virtual System Memory data provides basic performance statistics for the virtual machine. For example, if you notice that the Apparent CPU% and the Memory Balloon edvalues are above normal, this could indicate that there is a sizing issue – the host systemdoesn't have enough resources for its virtual machines.

Terminals

This category is only included for focus systems that are physical machines. Selecting this category displays information regarding the user account, IP address, whether a session is active and the number of active sessions.

4.4.3 Black Box Tool

Like the Dashboard tool, the Black Box tool allows you to review detailed system data for a specific point in time. The Black Box's added graph allows you to select a time point within the last 30 days on the graph, and then review detail data collected at that focus time(to keep the database at a manageable size, detailed data is only retained for 30 days). Clicking any data point on the Graphing Tool's graph will open the Black Box Tool.

The graph is pre-populated with Fault, App Focus, and Alarm milestones, and a % total CPU data series. From select data grids categories, you can choose metrics to add to the graph asa data series. Multiple graphs are overlaid, allowing you to easily view and compare related concerns.

The steps below describe how you might use Black Box as a diagnostic tool when a user callsthe help desk to report an issue.

Using the Time Settings, set the graph's window of time to match the time frame ofthe reported issue.

Review the Graph for any issues, such as any Fault and/or Alarm milestones.Hovering over a milestone displays its details.

Select the specific point in time within the last thirty days (Focus Time) for which youwould like to review detailed data. You can do this by clicking on a specific graph data point or by manually changing the Focus Time.

Select the categories of data you would like to review for the selected Focus Time.

From select categories, you can add additional data series to the graph that may be helpful in your diagnosis. As illustrated in the screen shot below, you may, for example, want to add a data series to the graph that has a value highlighted with red (indicating a critical level for the metric), or yellow (indicating a warning level).

Use the Advanced Graph Content Controls to determine how the data series or milestones display on the graph. For example, you can apply a statistical function toa data series, or you can change the data's units.

You can display two system data grids simultaneously with a different metric as shown below:

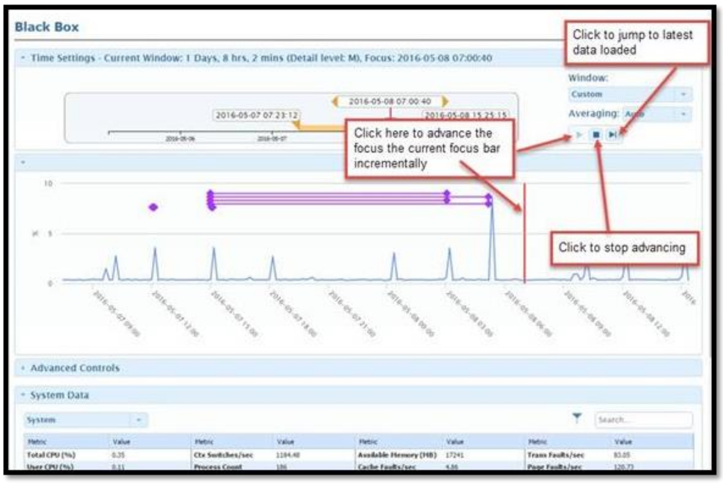
Adjust the Focus Time

The current date/time displayed reflects the focus time for the tool's data – allowing you to use the system status display (data grid) to review what was happening on the system at the specific point in time as well as change the date and time range.

If you change the focus time in the System Dashboard, it is changed in the Black Box.

Use the following methods to change the focus time:

1. Drag the entire orange bar
2. Pull and drag either end of the orange bar to change the end or start date/time
3. Drag the bottom of the red arrow to change to current focus time (available on the System Dashboard and Black Box)
4. Manually change the start, focus, or end date/time by placing your cursor in one of the three date/ time fields to display a blue highlight. Then enter the desired focus time. When you are done, you must click outside of the field for your change to take effect.
5. Select a time frame from the **Window** drop-down field (default is Custom).



Black Box

Time Settings - Current Window: 1 Days, 8 hrs, 2 mins (Detail level: M), Focus: 2016-05-08 07:00:40

Window: Custom

Averaging: Auto

Click to jump to latest data loaded

Click here to advance the focus the current focus bar incrementally

Click to stop advancing

Metric	Value	Metric	Value	Metric	Value	Metric	Value
Total CPU (%)	0.35	Ctx Switches/sec	1184.48	Available Memory (MB)	17241	Trans Faults/sec	83.05
User CPU (%)	0.11	Process Count	186	Cache Faults/sec	4.86	Page Faults/sec	120.73

6. Use the load function buttons to advance the current focus incrementally.
7. Select the Averaging Setting.

The Averaging Setting controls how the raw data points are treated before being graphed. If **Auto** is selected, the raw data points are graphed without being altered if there are not too many points to graph (high detail and/or long window time). The maximum number of points that can be graphed is 500. The chart averages the points so that they meet the 500-point maximum. If the setting is anything other than Auto, the data is averaged into periods as defined by the setting. For example, if the Averaging setting is 1 HR and the time window is the last 24 hours, there will be 24 data points graphed. If the raw data is at a higher sample rate than 1 hour, the points occurring in each hour are averaged to get the value for that hour's data point.

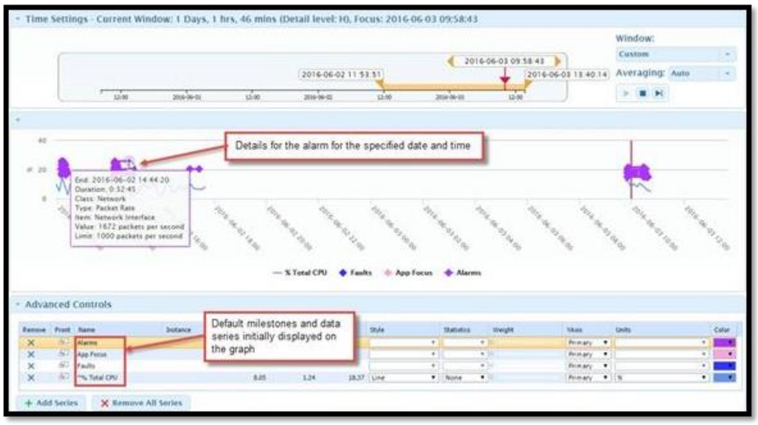
When a series is being averaged (because of too many points or a manual setting), a *proceeds the series name.

Black Box Graph

The Time Settings allow you to determine the window of time for the graph. The Graph has the following set of default milestones and data series:

- Faults
- App Focus
- Alarms
- % Total CPU

Hovering over a data point, such as an Alarm milestone, displays its details for the specified date and time. The alarm milestones (and corresponding details) are color coded. Red alarm milestones indicate critical level alarms; yellow alarm milestones indicate warning level alarms.



Time Settings - Current Window: 1 Days, 1 hrs, 46 mins (Detail level: H), Focus: 2016-06-03 09:58:43

Window: Custom

Averaging: Auto

End: 2016-06-02 14:44:20
Duration: 0:32:45
Class: Network
Type: Packet Rate
Item: Network Interface
Value: 1672 packets per second
Limit: 1000 packets per second

Details for the alarm for the specified date and time

Advanced Controls

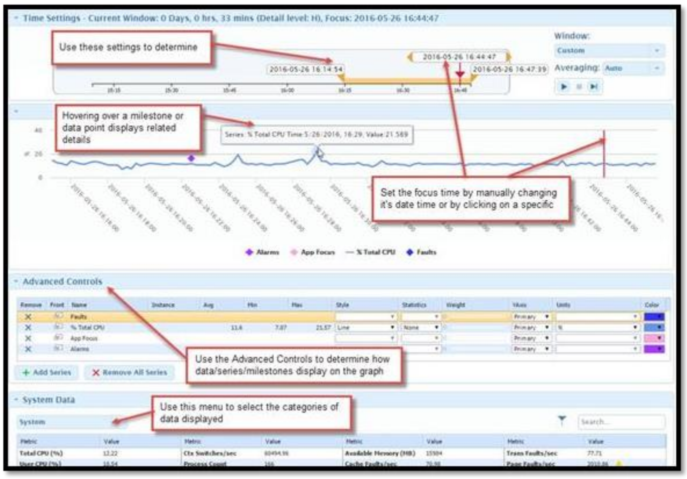
Default milestones and data series initially displayed on the graph

Remove	Pivot	Name	Instance				Style	Statistics	Weight	Y-Axis	Units	Color
✕		Alarms								Primary		
✕		App Focus								Primary		
✕		Faults								Primary		
✕		*% Total CPU		8.05	1.24	18.37	Line	None		Primary	%	

Clicking on a graph data point that falls within the last 30 days selects the specific point intime (the Focus Time) for which you would like to review detailed data (to keep the database at a manageable size, detailed data is only retained for 30 days).

You can select metrics to add to the graph as a data series. Any series you add persiststhroughout your current Device Lookup session.

Categorized Data Grids



Time Settings - Current Window: 0 Days, 0 hrs, 33 mins (Detail level: H), Focus: 2016-05-26 16:44:47

Use these settings to determine

Hovering over a milestone or data point displays related details

Series: % Total CPU Time 5/26/2016, 16:29, Value 21.589

Set the focus time by manually changing it's date time or by clicking on a specific

Use the Advanced Controls to determine how data/series/milestones display on the graph

Use this menu to select the categories of data displayed

The Black Box Tool's two data grids allow you to compare two different categories of detailed data that was gathered at a specific point in time (the Focus Time) within the last 30 days (to keep the database at a manageable size, detailed data is only retained for 30 days). To select the data categories, click the drop-down menu at the top of the System Data grid, and select the desired data category from the list. The Black Box Tool uses the same data categories as the Dashboard Tool.

You can select metrics to add to the graph as a data series. Any series you add persists throughout your current Device Lookup session. See Adding a Data Series to the Black Box Graph for more information.

Add a Data Series to the Graph

From select data grid categories, you can choose metrics to add to the graph as a dataseries. Any series you add persists throughout your current Device Lookup session.

Once you have added a data series to the graph, you can use the Advanced Graph ContentControls for functionality such as changing the series' graphical style or units.

To add a data series to the graph:

8. In the **Advanced Controls** pane, click the **Add Series** button.
9. From the Add Series dialog, click to select the metric(s) you want to add to the graphas a data series. The selected metric is added to the Advanced Controls table and graph as a dataseries.
10. To remove a series from the graph, click the X to the left of the metric in the Advanced Controls table that you wish to remove.
11. If you wish to remove all the series listed in the Advanced Controls table, click **Remove All Series**.

You can also add certain metrics from the System Data grid to the graph.

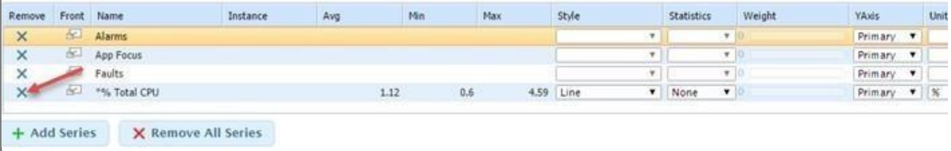
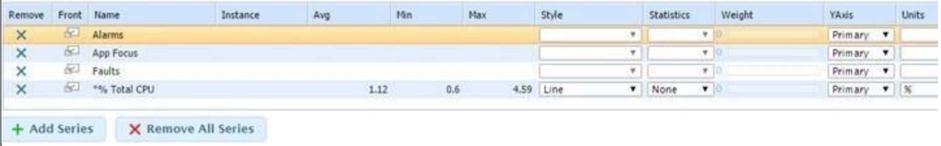
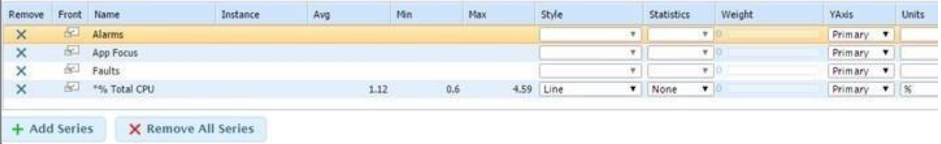
Add Metrics to the Black Box Graph

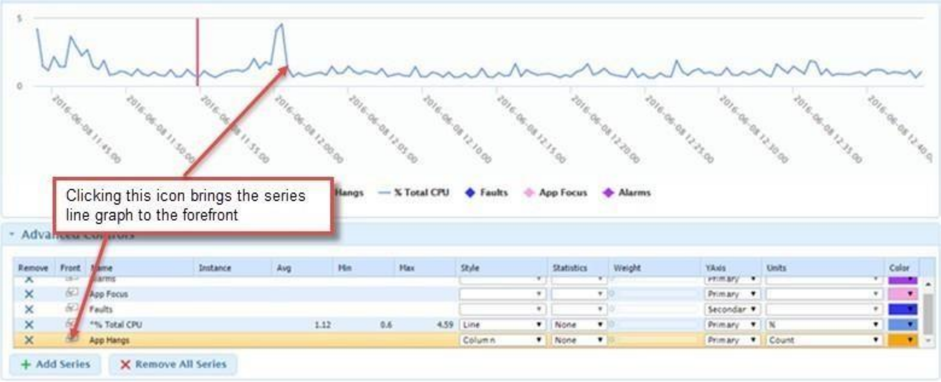
You can add metrics from the System Data grid to the Black Box graph from the System,Application, or Disk categories by clicking on a value for the metric. The Value turns orange when you hover over it, indicating that it can be added to the graph.

Advanced Graph Content Controls

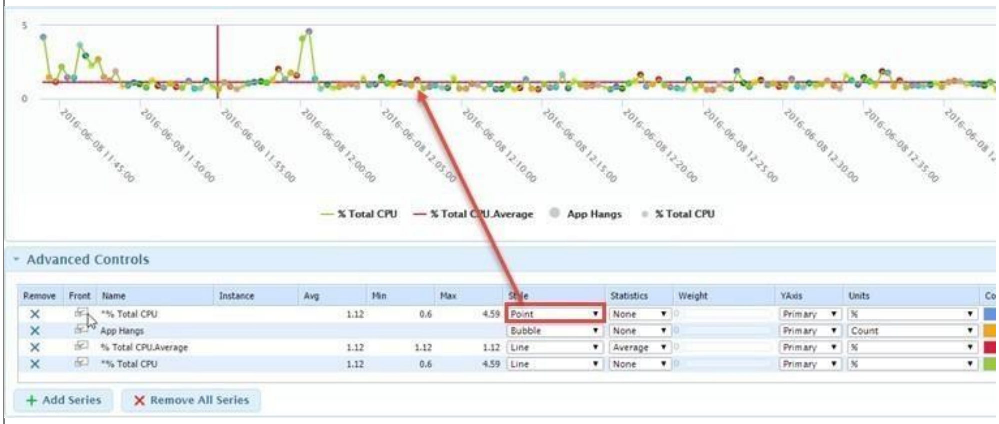
The following table describes each of the available Advanced Graph Content Controls:

Control	Description

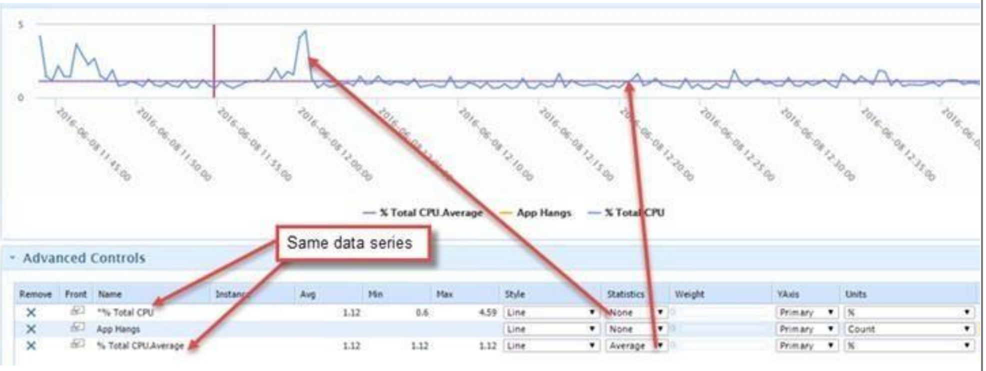
<table>
<tr>
<td>✕</td>
<td>This control icon removes a data series from the graph.

<table>
<tr><th>Remove</th><th>Front</th><th>Name</th><th>Instance</th><th>Avg</th><th>Min</th><th>Max</th><th>Style</th><th>Statistics</th><th>Weight</th><th>YAxis</th><th>Unit</th></tr>
<tr><td>✕</td><td></td><td>Alarms</td><td></td><td></td><td></td><td></td><td></td><td></td><td>0</td><td>Primary</td><td></td></tr>
<tr><td>✕</td><td></td><td>App Focus</td><td></td><td></td><td></td><td></td><td></td><td></td><td>0</td><td>Primary</td><td></td></tr>
<tr><td>✕</td><td></td><td>Faults</td><td></td><td></td><td></td><td></td><td></td><td></td><td>0</td><td>Primary</td><td></td></tr>
<tr><td>✕</td><td></td><td>*% Total CPU</td><td></td><td>1.12</td><td>0.6</td><td>4.59</td><td>Line</td><td>None</td><td>0</td><td>Primary</td><td>%</td></tr>
</table>
+ Add Series ✕ Remove All Series</td>
</tr>
<tr>
<td>✕ Remove All Series</td>
<td>This control icon removes all the data series from the graph.

<table>
<tr><th>Remove</th><th>Front</th><th>Name</th><th>Instance</th><th>Avg</th><th>Min</th><th>Max</th><th>Style</th><th>Statistics</th><th>Weight</th><th>YAxis</th><th>Units</th></tr>
<tr><td>✕</td><td></td><td>Alarms</td><td></td><td></td><td></td><td></td><td></td><td></td><td>0</td><td>Primary</td><td></td></tr>
<tr><td>✕</td><td></td><td>App Focus</td><td></td><td></td><td></td><td></td><td></td><td></td><td>0</td><td>Primary</td><td></td></tr>
<tr><td>✕</td><td></td><td>Faults</td><td></td><td></td><td></td><td></td><td></td><td></td><td>0</td><td>Primary</td><td></td></tr>
<tr><td>✕</td><td></td><td>*% Total CPU</td><td></td><td>1.12</td><td>0.6</td><td>4.59</td><td>Line</td><td>None</td><td>0</td><td>Primary</td><td>%</td></tr>
</table>
+ Add Series ✕ Remove All Series</td>
</tr>
<tr>
<td>+ Add Serie</td>
<td>
<table>
<tr><th>Remove</th><th>Front</th><th>Name</th><th>Instance</th><th>Avg</th><th>Min</th><th>Max</th><th>Style</th><th>Statistics</th><th>Weight</th><th>YAxis</th><th>Units</th></tr>
<tr><td>✕</td><td></td><td>Alarms</td><td></td><td></td><td></td><td></td><td></td><td></td><td>0</td><td>Primary</td><td></td></tr>
<tr><td>✕</td><td></td><td>App Focus</td><td></td><td></td><td></td><td></td><td></td><td></td><td>0</td><td>Primary</td><td></td></tr>
<tr><td>✕</td><td></td><td>Faults</td><td></td><td></td><td></td><td></td><td></td><td></td><td>0</td><td>Primary</td><td></td></tr>
<tr><td>✕</td><td></td><td>*% Total CPU</td><td></td><td>1.12</td><td>0.6</td><td>4.59</td><td>Line</td><td>None</td><td>0</td><td>Primary</td><td>%</td></tr>
</table>
+ Add Series ✕ Remove All Series</td>
</tr>
</table>

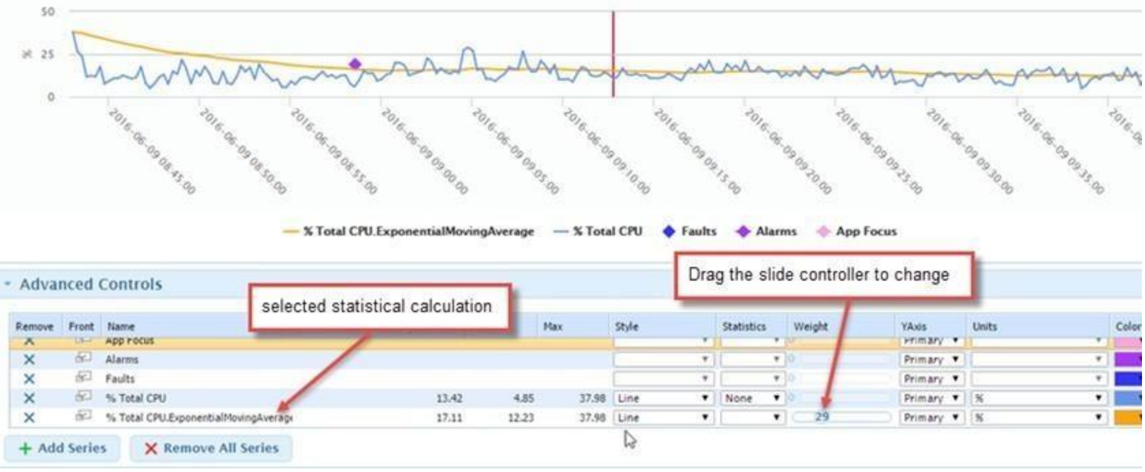
<table>
<tr>
<td>⧉</td>
<td>This control icon moves the series to the foreground of the graph. This control is especially useful if there are series with data points overlaying each other on the graph.

Clicking this icon brings the series line graph to the forefront

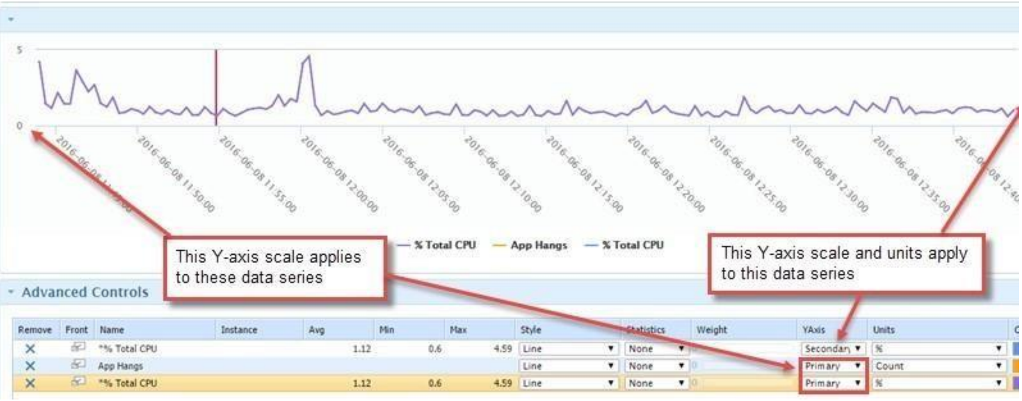
<table>
<tr><th>Remove</th><th>Front</th><th>Name</th><th>Instance</th><th>Avg</th><th>Min</th><th>Max</th><th>Style</th><th>Statistics</th><th>Weight</th><th>YAxis</th><th>Units</th><th>Color</th></tr>
<tr><td>✕</td><td>⧉</td><td>arms</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>Primary</td><td></td><td>🟪</td></tr>
<tr><td>✕</td><td>⧉</td><td>App Focus</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>Primary</td><td></td><td>🟪</td></tr>
<tr><td>✕</td><td>⧉</td><td>Faults</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>Secondar</td><td></td><td>🟦</td></tr>
<tr><td>✕</td><td>⧉</td><td>*% Total CPU</td><td></td><td>1.12</td><td>0.6</td><td>4.59</td><td>Line</td><td>None</td><td>0</td><td>Primary</td><td>%</td><td>🟦</td></tr>
<tr><td>✕</td><td>⧉</td><td>App Hangs</td><td></td><td></td><td></td><td></td><td>Column</td><td>None</td><td>0</td><td>Primary</td><td>Count</td><td>🟧</td></tr>
</table>
</td>
</tr>
<tr>
<td>Style</td>
<td>Allows you to change how a series is presented in the graph. For examp le, by changing the Style selection from <b>Line</b> to <b>Point</b>, data
points displayed as a line are changed to individual points. When multiple series are graphed, the list of <b>Style</b> options is filtered to those that are</td>
</tr>
</table>

<table>
<tr><th>Control</th><th>Description</th></tr>
<tr>
<td></td>
<td>

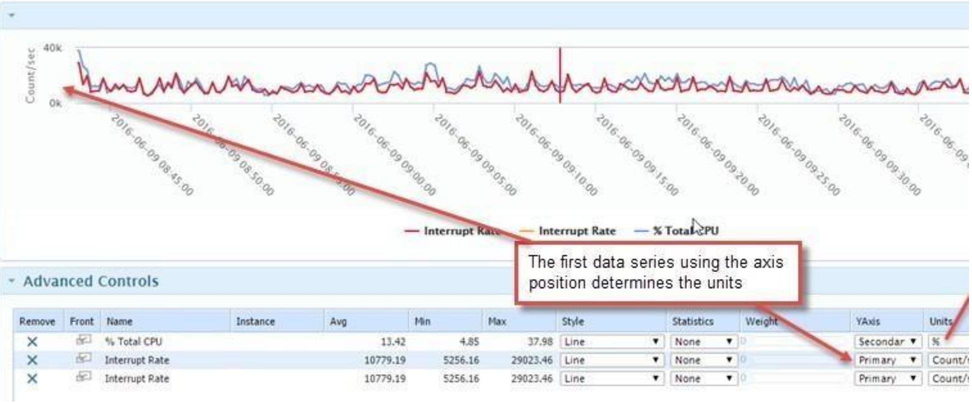
<table>
<tr><th>Remove</th><th>Front</th><th>Name</th><th>Instance</th><th>Avg</th><th>Min</th><th>Max</th><th>Style</th><th>Statistics</th><th>Weight</th><th>YAxis</th><th>Units</th><th>Co</th></tr>
<tr><td>✕</td><td>⧉</td><td>*% Total CPU</td><td></td><td>1.12</td><td>0.6</td><td>4.59</td><td>Point</td><td>None</td><td>0</td><td>Primary</td><td>%</td><td>🟦</td></tr>
<tr><td>✕</td><td>⧉</td><td>App Hangs</td><td></td><td></td><td></td><td></td><td>Bubble</td><td>None</td><td>0</td><td>Primary</td><td>Count</td><td>🟧</td></tr>
<tr><td>✕</td><td>⧉</td><td>% Total CPU.Average</td><td></td><td>1.12</td><td>1.12</td><td>1.12</td><td>Line</td><td>Average</td><td>0</td><td>Primary</td><td>%</td><td>🟥</td></tr>
<tr><td>✕</td><td>⧉</td><td>*% Total CPU</td><td></td><td>1.12</td><td>0.6</td><td>4.59</td><td>Line</td><td>None</td><td>0</td><td>Primary</td><td>%</td><td>🟩</td></tr>
</table>
compatible with the type selected for the first series.</td>
</tr>
</table>

Statistics	If you select a value other than **None**, a copy of the data set is made and a dded to the graph with the chosen statistical function applied to the copy.  % Total CPU.Average App Hangs % Total CPU Advanced Controls Same data series Remove | Front | Name | Instance | Avg | Min | Max | Style | Statistics | Weight | YAxis | Units ✕ | | *% Total CPU | | 1.12 | 0.6 | 4.59 | Line | None | 0 | Primary | % ✕ | | App Hangs | | | | | Line | None | 0 | Primary | Count ✕ | | % Total CPU.Average | | 1.12 | 1.12 | 1.12 | Line | Average | 0 | Primary | %
Weight	The weight value is a value used as a factor select statistical calculations. It can be applied to the following statistical calculations: Bollinger, Exponential Moving Average; ModifiedMoving Average; Simple **Moving Average**; **Weighted Moving Average**; **Momentum**; **Momentum Division**; and **Power**. You use the **Weight** slider to select the weight factor - ranging from 1 - 100%. The value that it modifies varies with the statistical calculation selected. For most calculations, it scales the count of points in the data set to be graphed and uses the scaledvalue as the factor in the statical calculation.

Cont rol	**Description**
	 50 % 25 0 % Total CPU.ExponentialMovingAverage % Total CPU Faults Alarms App Focus Advanced Controls + Add Series ✕ Remove All Series Drag the slide controller to change selected statistical calculation Remove | Front | Name | Max | Style | Statistics | Weight | YAxis | Units | Color ✕ | | App Focus | | | | | Primary | | ✕ | | Alarms | | | | 0 | Primary | | ✕ | | Faults | | | | 0 | Primary | | ✕ | | % Total CPU | 13.42 | 4.85 | 37.98 | Line | None | 0 | Primary | % ✕ | | % Total CPU.ExponentialMovingAverag | 17.11 | 12.23 | 37.98 | Line | | 29 | Primary | %

<table>
<tr><td>Y Axis</td><td>Controls which axis position the series Y data is charted on. When <b>Primary</b> is selected, the scale on the <i>left</i> side of the chart applies to the series.
When <b>Secondary</b> is selected, the scale on the <i>right</i> side of the chart applies to the series.


This Y-axis scale applies to these data series
This Y-axis scale and units apply to this data series
<table>
<tr><th>Remove</th><th>Front</th><th>Name</th><th>Instance</th><th>Avg</th><th>Min</th><th>Max</th><th>Style</th><th>Statistics</th><th>Weight</th><th>YAxis</th><th>Units</th></tr>
<tr><td>✕</td><td></td><td>*% Total CPU</td><td></td><td>1.12</td><td>0.6</td><td>4.59</td><td>Line</td><td>None</td><td></td><td>Secondary</td><td>%</td></tr>
<tr><td>✕</td><td></td><td>App Hangs</td><td></td><td></td><td></td><td></td><td>Line</td><td>None</td><td>0</td><td>Primary</td><td>Count</td></tr>
<tr><td>✕</td><td></td><td>*% Total CPU</td><td></td><td>1.12</td><td>0.6</td><td>4.59</td><td>Line</td><td>None</td><td>0</td><td>Primary</td><td>%</td></tr>
</table></td></tr>
<tr><td>Units</td><td>The units being used for the data series. Depending on the data, you may be able to select different units for the series if the initial units can be easily converted. When more than one series shares a Y axis position (Primary or Secondary), the first series added to that position will determine which units are used, but the scale will encompass the values from all series.</td></tr>
</table>

<table>
<tr><th>Control</th><th>Description</th></tr>
<tr><td></td><td>

The first data series using the axis position determines the units
<table>
<tr><th>Remove</th><th>Front</th><th>Name</th><th>Instance</th><th>Avg</th><th>Min</th><th>Max</th><th>Style</th><th>Statistics</th><th>Weight</th><th>YAxis</th><th>Units</th></tr>
<tr><td>✕</td><td></td><td>% Total CPU</td><td></td><td>13.42</td><td>4.85</td><td>37.98</td><td>Line</td><td>None</td><td>0</td><td>Secondar</td><td>%</td></tr>
<tr><td>✕</td><td></td><td>Interrupt Rate</td><td></td><td>10779.19</td><td>5256.16</td><td>29023.46</td><td>Line</td><td>None</td><td>0</td><td>Primary</td><td>Count/</td></tr>
<tr><td>✕</td><td></td><td>Interrupt Rate</td><td></td><td>10779.19</td><td>5256.16</td><td>29023.46</td><td>Line</td><td>None</td><td>0</td><td>Primary</td><td>Count/</td></tr>
</table></td></tr>
<tr><td>Color</td><td>The color used to render the series data on the graph. This column can act asa color key for the graph's series.</td></tr>
</table>

4.4.4 Health Tool

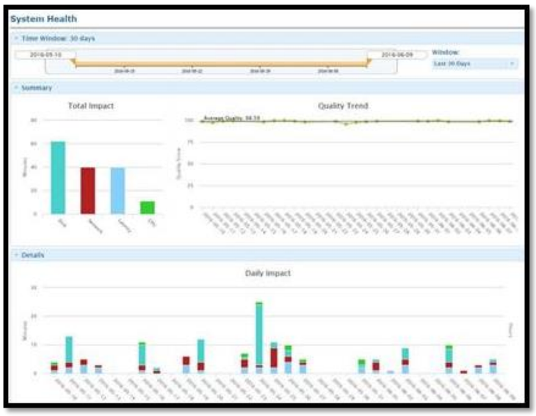
The Health tool provides a look at the system's health score (the service quality) over the past thirty days. Device Lookup's health score is easily compared to trending data from FleetView, which maintains up to three years of history.

After selecting a system, this is a good place to start looking for issues. For example, if a usercalls the help desk to report that their system is slow, using this tool you can quickly answer questions such as: how long ago did the service quality begin to decline? Or is there a continuous negative impact or a sporadic impact?

If you notice that an element has a high level of impact on the system's health, you use other Device Lookup tools to further research the issue. For example, if the Health tool indicates that application faults are having a high impact on system health, you could usethe Black Box tool to determine which applications were active during the point in time when faults were having the highest impact on the system health.

The tool is comprised of the following components:

- Time Window
- Total Impact Chart
- Quality Trend Line Graph



Daily Impact Bar Graph

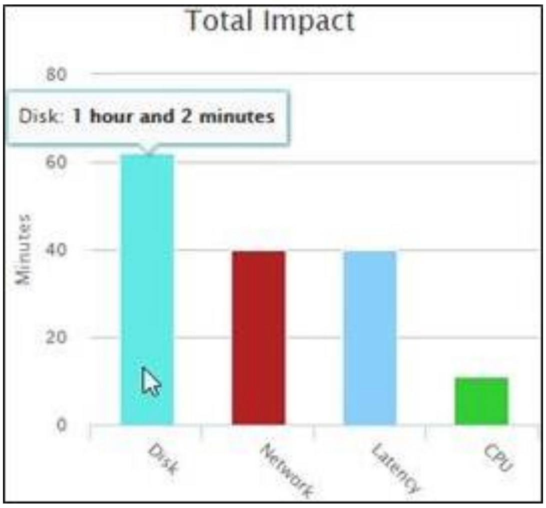
Time Window

The Time Window allows you to select a time frame to display in the following ways:

- Select a time frame from the **Window** drop-down list (default is Last 30 days)
- Drag either end of the orange bar to change the start and end times or dragthe entire orange bar.

Manually change the start and end times by placing your cursor in the start or end fields to display a blue highlight. Next enter the desired focus time. When you are finished, you must click outside of the field for your change to take effect.

Total Impact Chart

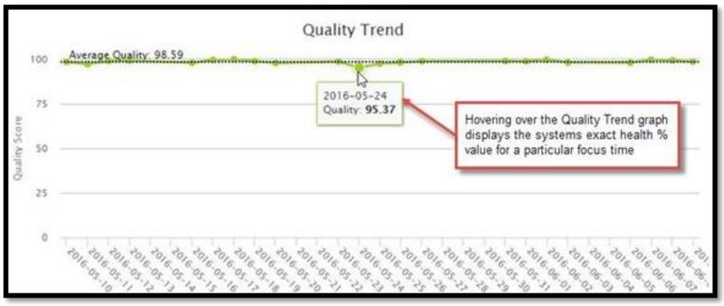


The Total Impact chart breaks out the categories that have impacted the system's performance. The value displayed for each category is the total number of minutes the category has impacted the system's performance over the last 30 days. Although the Disk category in the following chart contributes the most by far to the system's health impact, you need to consider the Quality Trend to put it into context.

Quality Trend

The line graph provides a quality trend over the focus time. The closer the QualityTrend is to 100%, the closer the system is to perfect performance health.

The example Health Tool screen shots in this topic are for a physical desktop. As illustrated by the example Quality Trend shown below, it is common for physical desktops to have very good performance health.

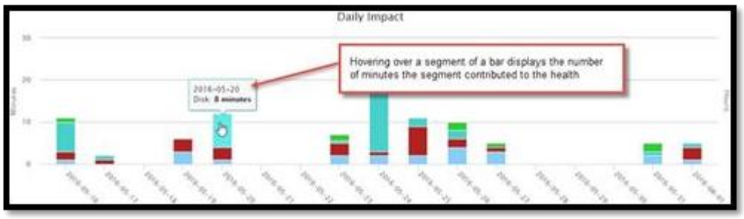


Hovering over the Quality Trend graph displays the systems exact health % value for a particular focus time

Daily Impact Bar Graph

Both the 30-Day Impact pie chart and this bar graph break out the categories that have impacted the system's performance. While the 30-Day Impact pie chart provides the totalnumber of minutes the category has impacted the system's performance over the last 30 days, this bar chart shows the impact minutes for each category over time.

The bars at each date point are broken into color coded category segments. Hover over acategory segment to display the category's impact minutes for the indicated date.



Hovering over a segment of a bar displays the number of minutes the segment contributed to the health

4.4.5 System Usage

The System Usage Tool provides a graphical summary of the system's utilization over the last thirty days. The tool is comprised of the following components:

- Time Window
- System Usage Pie Chart
- Active App Focus Pie Chart
- Active Web Sites Focus Pie Chart
- Application Focus Over Time Bar Graph
- Website Focus Over Time Bar Graph

Time Window

The Time Window allows you to select a time frame to display in the following ways:Select a time frame from the Window drop-down menu (default is **Last 30 days**).

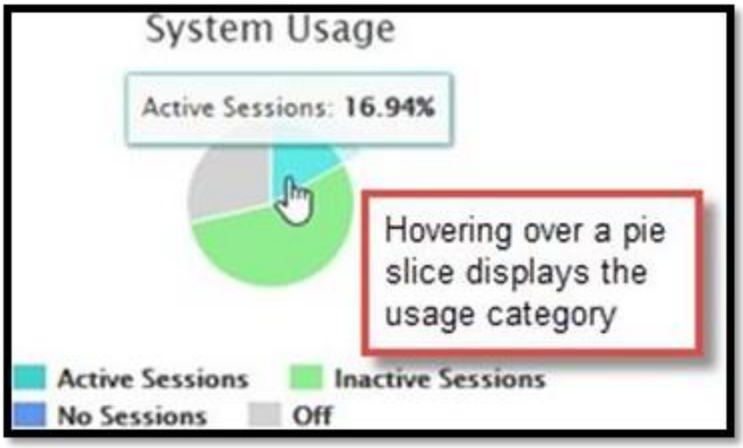
Drag the either end of the orange bar to change the start and end times or drag the entireorange bar.

Manually change the start and end times by placing your cursor in the start or end fields todisplay a blue highlight. Then enter the desired focus time. When you are done, you must click outside of the field for your change to take effect.

System Usage Pie Chart

This pie chart breaks out the categories of system usage for the selected focus time andprovides a usage percentage for each category.

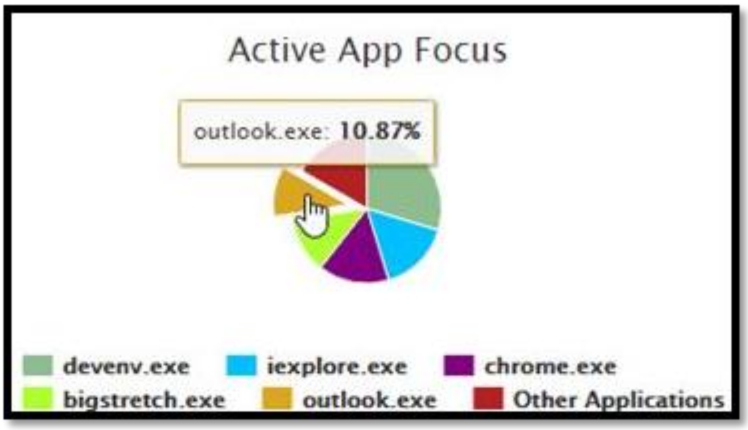
If a user does not turn their system off, there will be a sizeable percentage of time dedicated to Inactive Sessions.



Hovering over a pie slice displays the usage category

Active App Focus Pie Chart

This pie chart breaks out the applications that have been in use (while the system was active) for the selected focus time. You can quickly look at this chart and determine which applications are worked with most frequently.



4.4.6 Dependencies

This tool provides a system dependency map that includes a history of systems used to access the targeted system, local and mapped drives, and application dependencies and network latencies to and from dependent backend servers.

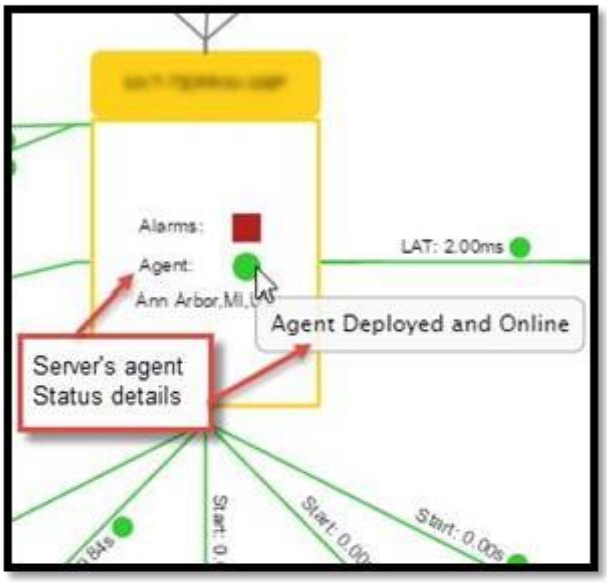
The dependency map is useful for tracking down problems. For example, a red dependency leg indicates an issue. If the map has any red legs, you use other Device Lookup tools to further investigate.

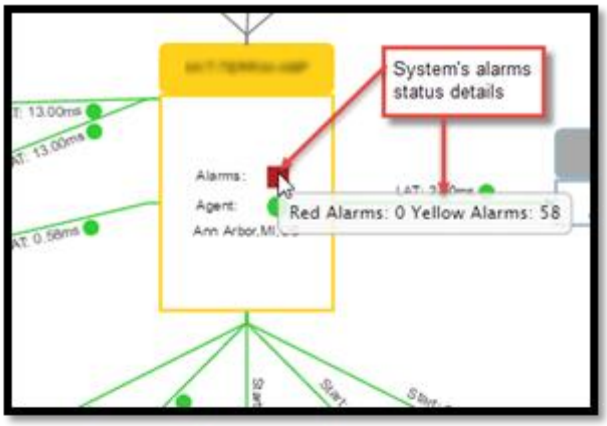
Latency (in milliseconds) is provided for individual dependencies. As labelled below, there is a low latency connection with the Default Gateway as you would expect.

In the example dependency map below, there is a slide control in the lower left corner (labelled **Dependencies from the last 3 days**). This slide allows you to adjust the time for the displayed application dependencies.

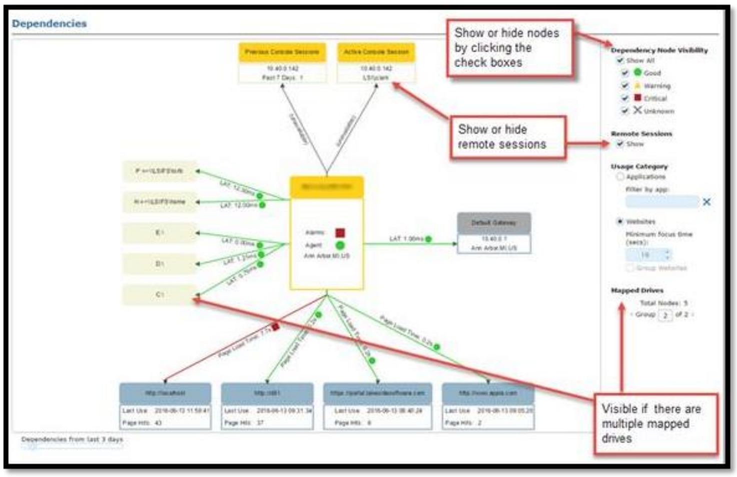
To zoom in and out on the Dependencies page, either use the scroll wheel on your mouse, or the + - keys on your keyboard.

As illustrated in the two screen shots below, hovering over the color-coded alarm and agent status icons displays details.




System's alarms status details
Alarms:
Agent:
Ann Arbor,MI,U
Red Alarms: 0 Yellow Alarms: 58
13.00ms
0.58ms

The controls on the right of the page that allow you to determine the type of dependenciesthat display.


Dependencies
Show or hide nodes by clicking the check boxes
Show or hide remote sessions
Visible if there are multiple mapped drives
Previous Console Sessions
Active Console Session
Default Gateway
LAT: 1.00ms
Alarms:
Agent:
Ann Arbor,MI,US
E:\
D:\
C:\
Page Load Time
Dependencies from last 3 days

Dependency Node Visibility
- ☑ Show All
- ☑ Good
- ☑ Warning
- ☑ Critical
- ☑ Unknown

Remote Sessions
- ☑ Show

Usage Category
- ○ Applications
- Filter by app:
- ● Websites
- Minimum focus time (secs): 10
- □ Group Websites

Mapped Drives
- Total Nodes: 5
- Group 2 of 2

Dependency Node Visibility

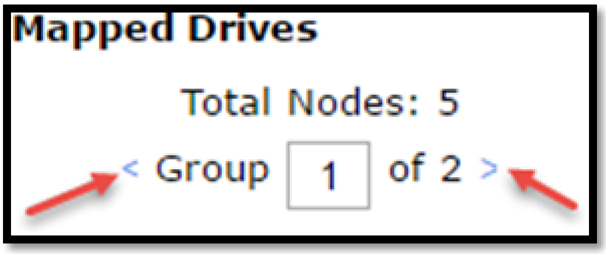
Shows or hides the various Dependency nodes (Show All, Good, Warning, Critical, or Unknown) by selecting the appropriate check boxes.

Usage Categories

- You can choose to view Applications or Websites by selecting the appropriate radio button in the **Usage Category** section.
- If you choose Applications, you have the option to filter by specific application. Key the name of the application to filter by (for example: chrome.exe).

Mapped Drives

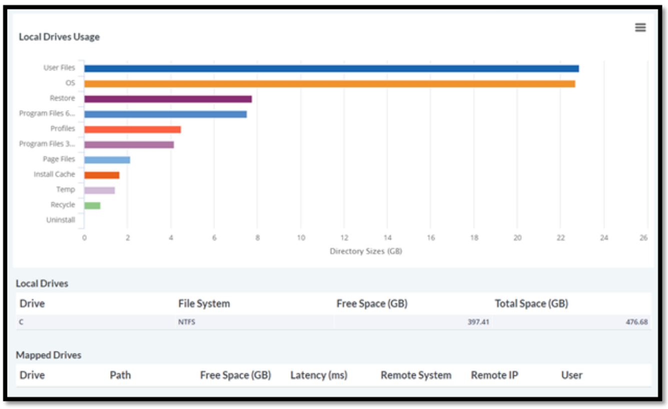
If the system has more than three mapped or local drives, a Mapped Drives control displays towards the lower right corner. Click the forward or back arrow to display the next or previous group of drives on the dependency map.



If you have employed more than eight methods of accessing their desktop, there are control towards the lower right corner that when clicked display the next group of access methods.

4.4.7 Hardware Tool

This tool provides an inventory of the system's hardware including a disk usage breakdown and information about both local and mapped drives.



Local Drives

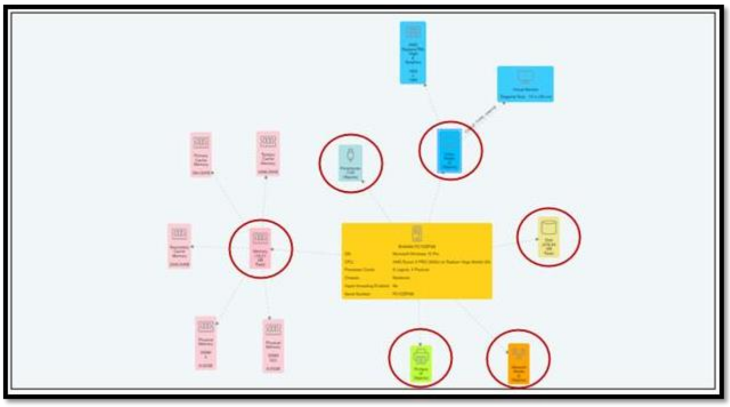
Drive	File System	Free Space (GB)	Total Space (GB)
C	NTFS	397.41	476.68

Mapped Drives

Drive	Path	Free Space (GB)	Latency (ms)	Remote System	Remote IP	User

4.4.8 Hardware Diagram Tool

The Hardware Diagram tool displays a categorization of all peripherals connected to a selected device. Click on a category card to view the detail of all peripherals. Click again on the category card to hide the listing of the peripherals.

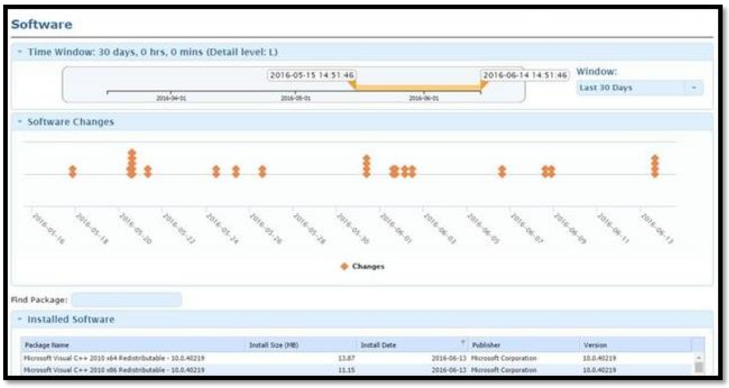


4.4.9 Software

This tool provides a history of software package changes, installations, and usage for the selected time. This tool is particularly useful to IT support personnel confronted with unauthorized changes on the system.

The tool is comprised of the following components:

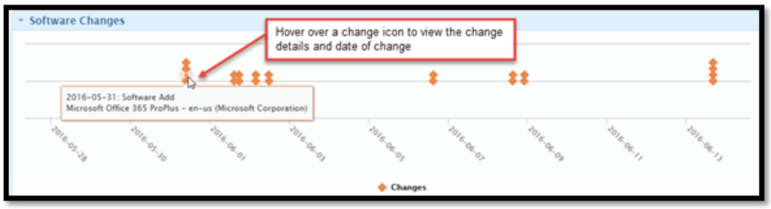
- Focus Time Selector
- Software Changes
- Installed Software
- Software Usage



Window: Last 30 Days

Package Name	Install Size (MB)	Install Date	Publisher	Version
Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219	13.87	2016-06-13	Microsoft Corporation	10.0.40219
Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219	11.15	2016-06-13	Microsoft Corporation	10.0.40219

Software Changes



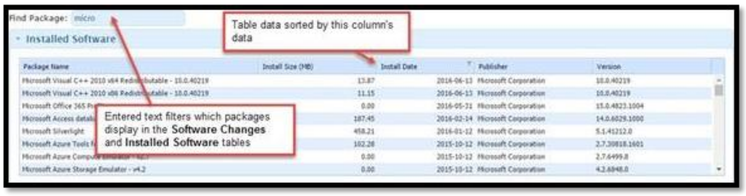
Hover over a change icon to view the change details and date of change

2016-05-31: Software Add
Microsoft Office 365 ProPlus – en-us (Microsoft Corporation)

Shows or hides the various Dependency nodes (Show All, Good, Warning, Critical, orUnknown) by selecting the appropriate check boxes.

Installed Software

This table provides information about the software packages that were installed during the selected time period. To filter which packages are included in the table, begin typing the name of the package in the Filter field. You can sort the table by a column's data by clicking on the column's header.



Find Package: micro

Installed Software

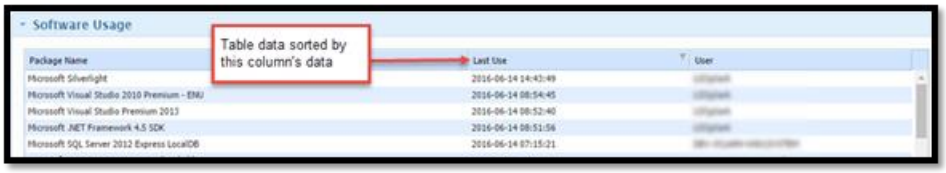
Table data sorted by this column's data

Entered text filters which packages display in the **Software Changes** and **Installed Software** tables

Package Name	Install Size (MB)	Install Date	Publisher	Version
Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219	13.87	2016-06-13	Microsoft Corporation	10.0.40219
Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219	11.15	2016-06-13	Microsoft Corporation	10.0.40219
Microsoft Office 365 Pr	0.00	2016-05-31	Microsoft Corporation	15.0.4823.1004
Microsoft Access datab	187.45	2016-02-14	Microsoft Corporation	14.0.6029.1000
Microsoft Silverlight	458.21	2016-01-12	Microsoft Corporation	5.1.41212.0
Microsoft Azure Tools f	102.28	2015-10-12	Microsoft Corporation	2.7.30818.1601
Microsoft Azure Compu - v2.7	0.00	2015-10-12	Microsoft Corporation	2.7.6499.8
Microsoft Azure Storage Emulator - v4.2	0.00	2015-10-12	Microsoft Corporation	4.2.6848.0

Software Usage

This table provides software usage data for the selected time period. The filter feature described above also filters this table. You can sort the table by a column's data by clicking on the column's header.

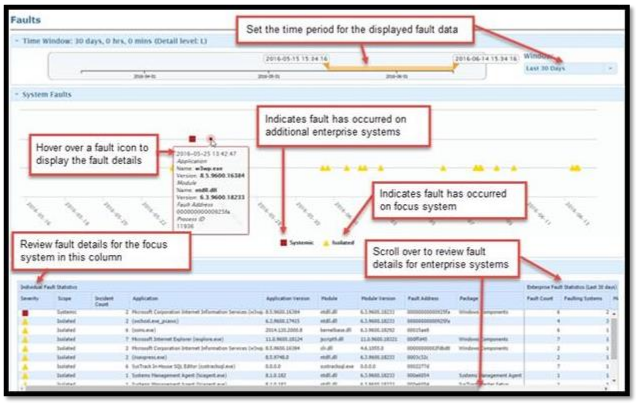


Software Usage

Table data sorted by this column's data

Package Name	Last Use	User
Microsoft Silverlight	2016-06-14 14:43:49	[redacted]
Microsoft Visual Studio 2010 Premium - ENU	2016-06-14 08:54:45	[redacted]
Microsoft Visual Studio Premium 2013	2016-06-14 08:52:40	[redacted]
Microsoft .NET Framework 4.5 SDK	2016-06-14 08:51:56	[redacted]
Microsoft SQL Server 2012 Express LocalDB	2016-06-14 07:15:21	[redacted]

4.4.10 Faults



Faults

Time Window: 30 days, 0 hrs, 0 mins (Detail level: L)

Set the time period for the displayed fault data

2016-05-15 15:34:16

2016-06-14 15:34:16

Window: Last 30 Days

System Faults

Indicates fault has occurred on additional enterprise systems

Hover over a fault icon to display the fault details

2016-05-25 13:42:47
Application
Name: **w3wp.exe**
Version: **8.5.9600.16384**
Module
Name: **ntdll.dll**
Version: **6.3.9600.18233**
Fault Address
00000000000925fa
Process ID
11936

Indicates fault has occurred on focus system

■ Systemic ▲ Isolated

Review fault details for the focus system in this column

Scroll over to review fault details for enterprise systems

Individual Fault Statistics | Enterprise Fault Statistics (Last 30 days)

Severity	Scope	Incident Count	Application	Application Version	Module	Module Version	Fault Address	Package	Fault Count	Faulting Systems

This tool identifies the software package faults that have impacted the system during the selected time. If the scope of the fault is Systemic, the fault has occurred on at leastone other system in the enterprise. If the scope of the fault is Isolated, the fault has only occurred on the focus system. It is a good practice to further investigate systemic faults.

Advanced Tools

The following table describes each of Device Lookup's Advanced Tools:

vanced Tool	Description
Boot/Logon Time	Provides boot and logon data for the last thirty days.
Logon Process	Provides system data relating to the reboot and logon process.
Event Correlation	Overlays fault events and alarms with any system changes made. Allows youto roll the system back to provided restore points.

All Inventory	Provides data for each of the system's existing inventory items.
Graphing	Generates graphs for selected system metrics and milestones over a specified time. Multiple graphs are overlaid, allowing you to easily view and compare related concerns.
Comparative Analytics	Allows you to compare selected metrics collected from the focus system metrics to the metrics of one or more groups of systems, with the option ofdisplaying threshold values for each selected metric.
File Information	Groups all files found on the focus system by file extension, and then providesfile age and file size data for each extension. The tool provides options that allow you to customize how the data is displayed.
Power Schedule	The Power Schedule displays power usage analysis for selected devices usingfour categories: Power Saving Hours, Power/Cooling Costs, Estimated Costs and Savings.
Tools	Tools gives the user the ability to run automations on a selected device. Automations include clearing the recycle bin and running scripts.

4.4.11 Boot/Logon Time Tool

The Boot/Logon Time Tool is not available for systems that have Application Hook setting disabled. Application Hook allows the collection of application start data required for the Boot/Logon Time Tool.

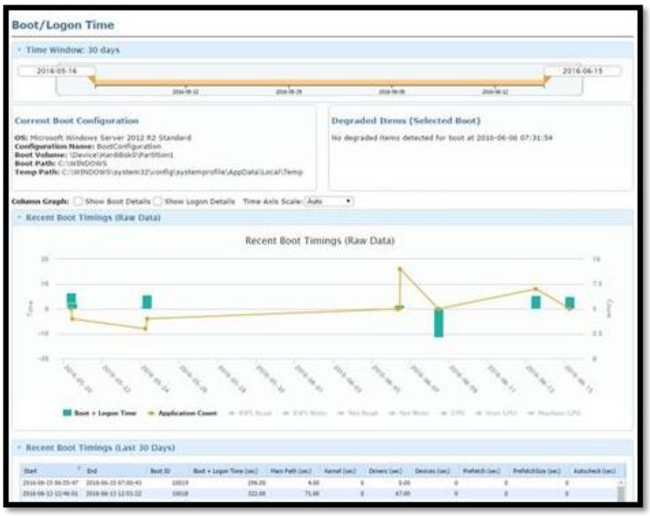
The Application Hook setting is applied to systems via the system's assigned Deployment Tool profile configuration. It is enabled or disabled via the configuration's Policies and Settings tab, in the Application Management category of policies.

This tool provides boot and logon data for the last thirty days. Using the data, you candetermine if there are any specific issues that are causing slower boot times.

Additionally, the tool's graph maps boot times to system login processes to assist in problem determination.

The tool is comprised of the following components:

- Focus Time Selector
- Current Boot Configuration
- Degraded Items (Selected Boot)
- Recent Boot Timings (Raw Data) Graph
- Recent Boot Timings (Raw Data) Table



Boot/Logon Time

Time Window: 30 days

2016-05-16 — 2016-06-15

Current Boot Configuration

OS: Microsoft Windows Server 2012 R2 Standard
Configuration Name: BootConfiguration
Boot Volume: \Device\Harddisk0\Partition1
Boot Path: C:\WINDOWS
Temp Path: C:\WINDOWS\system32\config\systemprofile\AppData\Local\Temp

Degraded Items (Selected Boot)

No degraded items detected for boot at 2016-06-06 07:31:54

Column Graph: □ Show Boot Details □ Show Logon Details Time Axis Scale: Auto

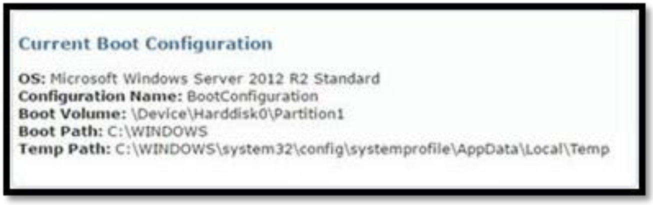
Recent Boot Timings (Raw Data)

Recent Boot Timings (Last 30 Days)

Start	End	Boot ID	Boot + Logon Time (sec)	Main Path (sec)	Kernel (sec)	Drivers (sec)	Devices (sec)	Prefetch (sec)	PrefetchSize (sec)	Autocheck (sec)
2016-06-15 06:55:47	2016-06-15 07:00:43	10019	296.00	4.00	0	3.00	0	0	0	0
2016-06-13 12:46:01	2016-06-13 12:51:22	10018	322.00	71.00	0	67.00	0	0	0	0

Current Boot Configuration

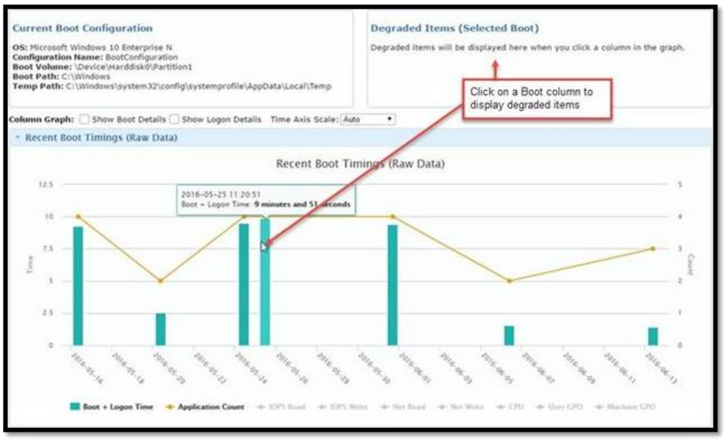
Provides the focus system's basic boot configuration information.



Current Boot Configuration

OS: Microsoft Windows Server 2012 R2 Standard
Configuration Name: BootConfiguration
Boot Volume: \Device\Harddisk0\Partition1
Boot Path: C:\WINDOWS
Temp Path: C:\WINDOWS\system32\config\systemprofile\AppData\Local\Temp

Degraded Items (Selected Boot)



Current Boot Configuration

OS: Microsoft Windows 10 Enterprise N
Configuration Name: BootConfiguration
Boot Volume: \Device\Harddisk0\Partition1
Boot Path: C:\Windows
Temp Path: C:\Windows\system32\config\systemprofile\AppData\Local\Temp

Degraded Items (Selected Boot)

Degraded items will be displayed here when you click a column in the graph.

Click on a Boot column to display degraded items

Column Graph: □ Show Boot Details □ Show Logon Details Time Axis Scale: Auto

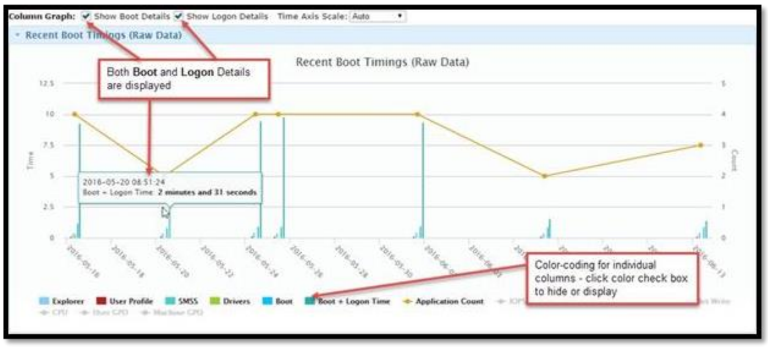
Recent Boot Timings (Raw Data)

2016-05-25 11:20:51
Boot + Logon Time: **9 minutes and 51 seconds**

Hovering over a bar chart on the graph displays any issues that caused slower boot times during the boot up in the **Degraded Items** pane.

Recent Boot Timings (Raw Data) Graph

Provides data in a graphical format for each system boot that has occurred for the selected Time Window (default is 30 days).



Column Graph: ☑ Show Boot Details ☑ Show Logon Details Time Axis Scale: Auto

Both **Boot** and **Logon** Details are displayed

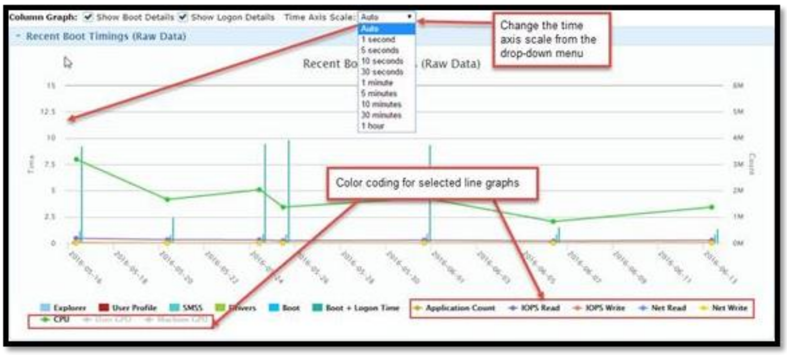
2016-05-20 08:51:24
Boot + Logon Time: **2 minutes and 31 seconds**

Color-coding for individual columns - click color check box to hide or display

You can opt to display **Boot Details** and **Logon Details** for the graph's boot and logon datapoints. Hovering over the individual components of a column displays the component's details.

Application Count is the default line graph. You can use the **Line Graph** check boxes tocontrol which line graphs display.

The scale/units on the left Y axis apply to the columns, and the scale on the right Y axis applies to the selected line graphs. When more than one line graph shares the right Y axis, the scale will encompass the highest and lowest values from each line graph.

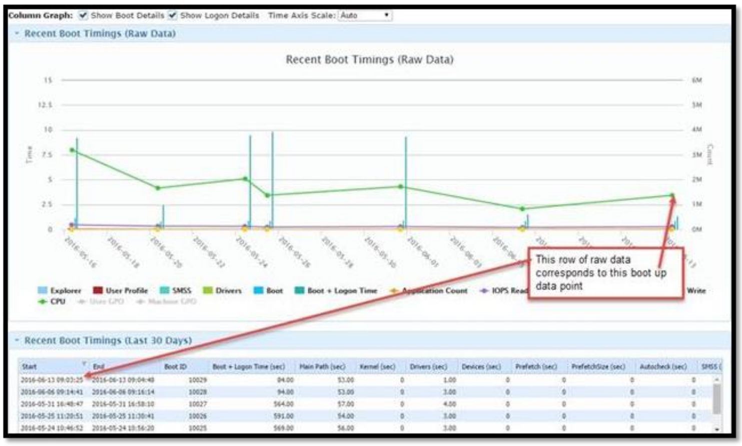


Column Graph: ☑ Show Boot Details ☑ Show Logon Details Time Axis Scale: Auto

Change the time axis scale from the drop-down menu

Color coding for selected line graphs

Recent Boot Timings (Raw Data) Table



Column Graph: ☑ Show Boot Details ☑ Show Logon Details Time Axis Scale: Auto

This row of raw data corresponds to this boot up data point

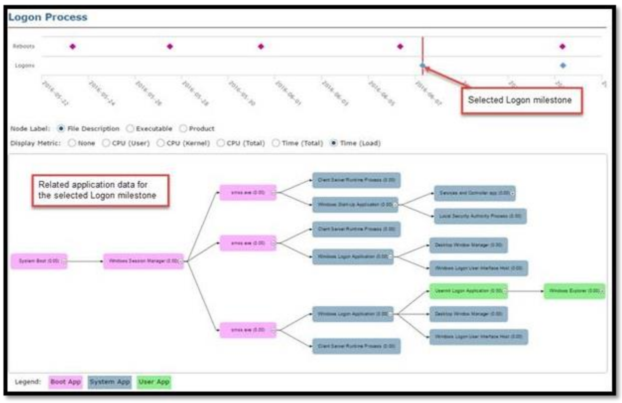
Recent Boot Timings (Last 30 Days)

Start	End	Boot ID	Boot + Logon Time (sec)	Main Path (sec)	Kernel (sec)	Drivers (sec)	Devices (sec)	Prefetch (sec)	PrefetchSize (sec)	Autocheck (sec)	SMSS (
2016-06-13 09:03:25	2016-06-13 09:04:48	10029	84.00	53.00	0	1.00	0	0	0	0	
2016-06-06 09:14:41	2016-06-06 09:16:14	10028	94.00	53.00	0	3.00	0	0	0	0	
2016-05-31 16:48:47	2016-05-31 16:58:10	10027	564.00	57.00	0	4.00	0	0	0	0	
2016-05-25 11:20:51	2016-05-25 11:30:41	10026	591.00	54.00	0	3.00	0	0	0	0	
2016-05-24 10:46:52	2016-05-24 10:56:20	10025	569.00	56.00	0	3.00	0	0	0	0	

The raw data for each of the Recent Boot Timing graph's data points is displayed in tabularformat.

4.4.12 Logon Process

The Logon Process Tool is not available for systems that have Application Hook setting disabled. Application Hook allows the collection of application start data required for theLogon Process Tool.


Logon Process
Reboots
Logons
2016-05-22
2016-05-24
2016-05-26
2016-05-28
2016-05-30
2016-06-01
2016-06-03
2016-06-05
2016-06-07
System Boot (0.00)
Windows Session Manager (0.00)
smss.exe (0.00)
Client Server Runtime Process (0.00)
Windows Start-Up Application (0.00)
Services and Controller app (0.00)
Local Security Authority Process (0.00)
Desktop Window Manager (0.00)
Windows Logon Application (0.00)
Windows Logon User Interface Host (0.00)
Userinit Logon Application (0.00)
Windows Explorer (0.00)
Legend:
Boot App
System App
User App

Selected Logon milestone

Node Label: ● File Description ○ Executable ○ Product

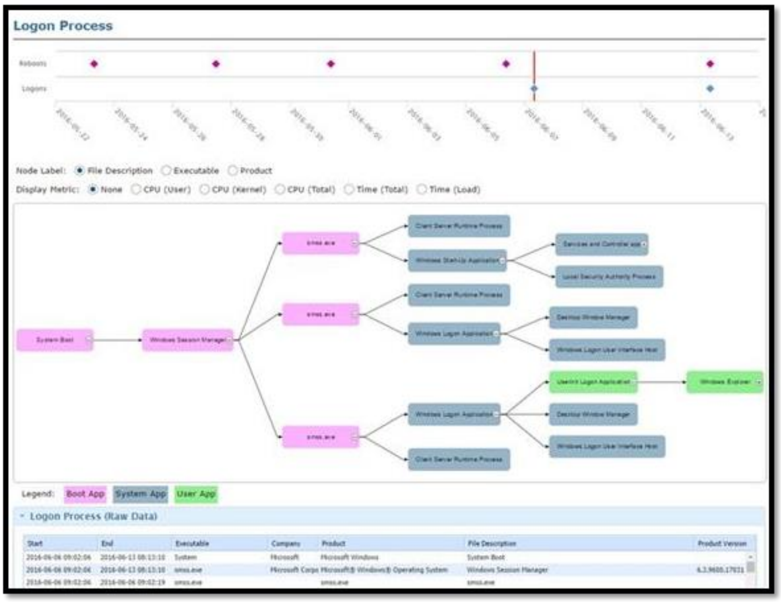
Display Metric: ○ None ○ CPU (User) ○ CPU (Kernel) ○ CPU (Total) ○ Time (Total) ● Time (Load)

Related application data for the selected Logon milestone

The Application Hook setting is applied to systems via the system's assigned Deployment Tool profile configuration. It is enabled/disabled via the configuration'sPolicies and Settings tab, in the Application Management category of policies.

This tool provides system data relating to the reboot and logon process. The tool iscomprised of the following components:

- Reboot and Logon Milestones
- Logon Process (Tree)
- Logon Process (Raw Data)


Logon Process
Reboots
Logons
System Boot
Windows Session Manager
smss.exe
Client Server Runtime Process
Windows Start-Up Application
Services and Controller app
Local Security Authority Process
Desktop Window Manager
Windows Logon Application
Windows Logon User Interface Host
Userinit Logon Application
Windows Explorer
Legend:
Boot App
System App
User App

Node Label: ● File Description ○ Executable ○ Product

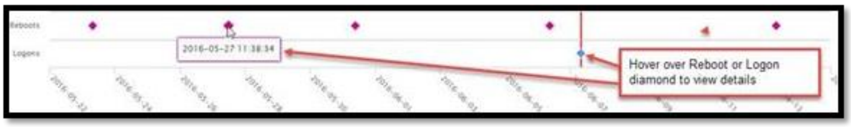
Display Metric: ● None ○ CPU (User) ○ CPU (Kernel) ○ CPU (Total) ○ Time (Total) ○ Time (Load)

Logon Process (Raw Data)

Start	End	Executable	Company	Product	File Description	Product Version
2016-06-06 09:02:06	2016-06-13 08:13:10	System	Microsoft	Microsoft Windows	System Boot	
2016-06-06 09:02:06	2016-06-13 08:13:10	smss.exe	Microsoft Corpo	Microsoft® Windows® Operating System	Windows Session Manager	6.3.9600.17031
2016-06-06 09:02:06	2016-06-06 09:02:19	smss.exe		smss.exe	smss.exe	

Reboot and Logon Milestones

The diamond icons on the Milestones chart represent system Reboots, Logons corresponding to their row in



Hover over Reboot or Logon diamond to view details

the chart. Hovering over an icon displays the time stamp for the event. A red line through a Logon diamond indicates that this is the area of focus for theLogon Process tree.

Selecting a logon milestone (click to select) displays the related application data for thelogon in the Logon Process Tree component.

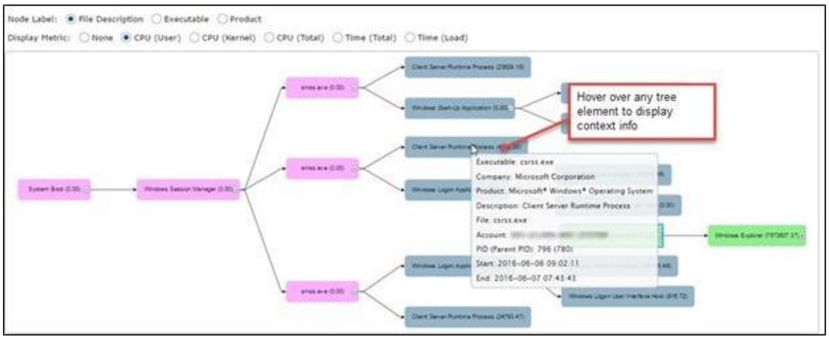
Logon Process (Tree)

The logon process tree initially displays application data for the current logon. To display related application data for a previous logon, click to select an earlier Logon Milestone.

Use the radio buttons to customize what displays on the tree elements. In the example shown below, the tree element labels display a description and the CPU (Total) statistic. The following table defines each of the available statistics.

Statistic	Definition
CPU (User)	CPU consumed by user mode processes.
CPU (Kernel)	CPU consumed by kernel mode processes.
CPU (Total)	Total CPU consumed by all processes (user and kernel mode).
Time (Total)	The total application execution time within the logon window. Metrics for applications that run past the end of the logon process are trimmed once the logon process is determined to be complete (this occurs at the point when the desktop is visible to the user and the system can respond to input). Device Lookup trims the metrics (like Time (Total), CPU, etc.) to show how much resource or how much time each application consumed in thelogon process.
Time (Load)	The time the process takes to initialize prior to informing the OS that it is running.

Hovering over a tree element displays context information for the element such as how longit took to start and how long it ran.



Node Label: ● File Description ○ Executable ○ Product

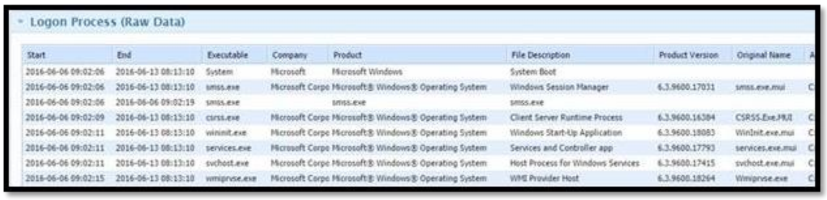
Display Metric: ○ None ● CPU (User) ○ CPU (Kernel) ○ CPU (Total) ○ Time (Total) ○ Time (Load)

Executable: csrss.exe
Company: Microsoft Corporation
Product: Microsoft® Windows® Operating System
Description: Client Server Runtime Process
File: csrss.exe
Account: [redacted]
PID (Parent PID): 796 (780)
Start: 2016-06-06 09:02:11
End: 2016-06-07 07:43:43

Hover over any tree element to display context info
System Boot (0.00)
Windows Session Manager (0.00)
smss.exe (0.00)
smss.exe (0.00)
smss.exe (0.00)
Windows Start-Up Application (0.00)
Windows Explorer

Logon Process (Raw Data)

The raw logon process data is initially sorted by Start time. Click any column header to sortthe data by that column's data.



Logon Process (Raw Data)

Start	End	Executable	Company	Product	File Description	Product Version	Original Name	A
2016-06-06 09:02:06	2016-06-13 08:13:10	System	Microsoft	Microsoft Windows	System Boot			
2016-06-06 09:02:06	2016-06-13 08:13:10	smss.exe	Microsoft Corpo	Microsoft® Windows® Operating System	Windows Session Manager	6.3.9600.17031	smss.exe.mui	C
2016-06-06 09:02:06	2016-06-06 09:02:19	smss.exe		smss.exe	smss.exe			
2016-06-06 09:02:09	2016-06-13 08:13:10	csrss.exe	Microsoft Corpo	Microsoft® Windows® Operating System	Client Server Runtime Process	6.3.9600.16384	CSRSS.Exe.MUI	C
2016-06-06 09:02:11	2016-06-13 08:13:10	wininit.exe	Microsoft Corpo	Microsoft® Windows® Operating System	Windows Start-Up Application	6.3.9600.18083	WinInit.exe.mui	C
2016-06-06 09:02:11	2016-06-13 08:13:10	services.exe	Microsoft Corpo	Microsoft® Windows® Operating System	Services and Controller app	6.3.9600.17793	services.exe.mui	C
2016-06-06 09:02:11	2016-06-13 08:13:10	svchost.exe	Microsoft Corpo	Microsoft® Windows® Operating System	Host Process for Windows Services	6.3.9600.17415	svchost.exe.mui	C
2016-06-06 09:02:15	2016-06-13 08:13:10	wmiprvse.exe	Microsoft Corpo	Microsoft® Windows® Operating System	WMI Provider Host	6.3.9600.18264	Wmiprvse.exe	C

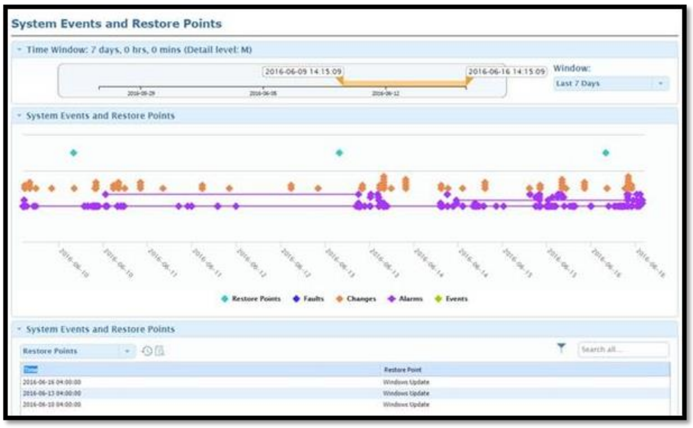
4.4.13 Event Correlation

This tool over lays fault events and system alarms with system changes that occurred during the same time frame. Additionally, this tool has an option that allows you to roll the system back to a point before the issues occurred.

Only Device Lookup users with administrative privileges for the focus system can perform a system roll back.

The tool is comprised of the following components:

- Time Settings
- System Events and Restore Points (Graph)
- System Events and Restore Points (Table)



System Events and Restore Points

Time Window: 7 days, 0 hrs, 0 mins (Detail level: M)

2016-06-09 14:15:09 – 2016-06-16 14:15:09

Window: Last 7 Days

System Events and Restore Points

System Events and Restore Points

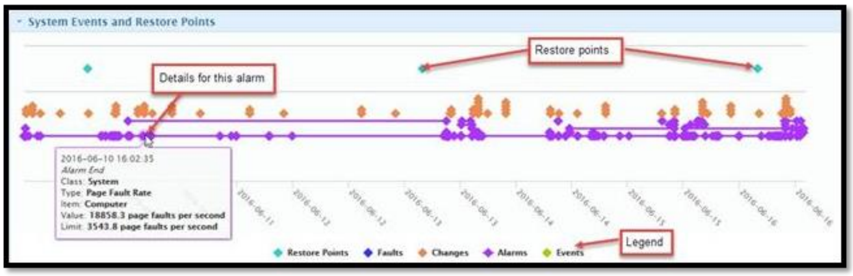
Restore Points

	Restore Point
2016-06-16 04:00:00	Windows Update
2016-06-13 04:00:00	Windows Update
2016-06-10 04:00:00	Windows Update

- Actions: Restore (Rolling Back the System to a Restore Point)

System Events and Restore Points Graph

The graph has icons for any system restore points, faults, changes, or alarms that occurduring the selected window of time. Hovering over each icon displays related details.



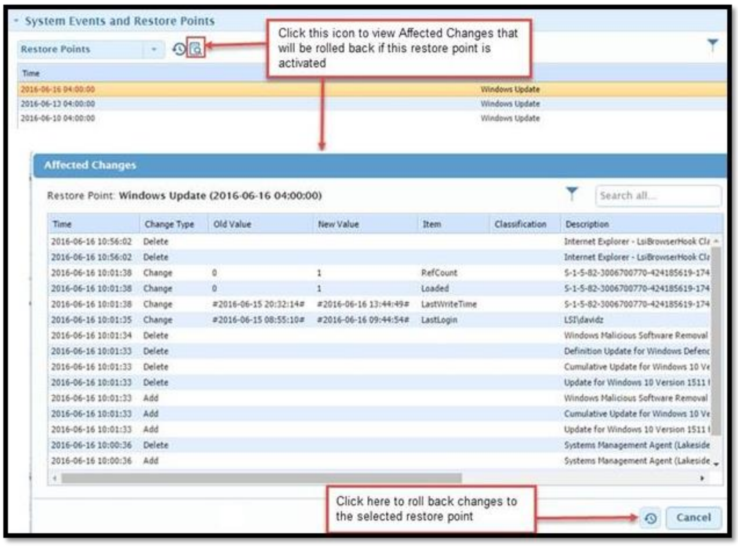
System Events and Restore Points

2016-06-10 16:02:35
Alarm End
Class: **System**
Type: **Page Fault Rate**
Item: **Computer**
Value: **18858.3 page faults per second**
Limit: **3543.8 page faults per second**

Hovering over a restore point icon displays system changes that are rolled back if you opt to restore the system to the restore point. Clicking each of the graph's diamonds displays data specific to the item in the System Events and Restore Points table.

System Events and Restore Points Table

The data initially displayed is associated with the latest restore point (the restore point with the most current time stamp). This data allows you to see which system changes are rolled back if you opt to restore the system to this restore point (these changes occurred after the restore point). You can sort the data by a column's data by clicking on that column's header. You can see the Affected Changes data for a different restore point by clicking affected changes icon as shown below.



Click this icon to view Affected Changes that will be rolled back if this restore point is activated

Time		Restore Point
2016-06-16 04:00:00		Windows Update
2016-06-13 04:00:00		Windows Update
2016-06-10 04:00:00		Windows Update

Restore Point: **Windows Update (2016-06-16 04:00:00)**

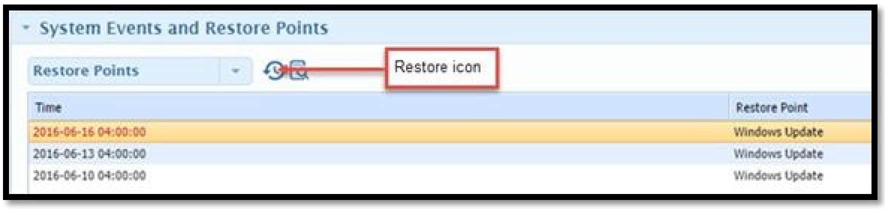
Time	Change Type	Old Value	New Value	Item	Classification	Description
2016-06-16 10:56:02	Delete					Internet Explorer - LsiBrowserHook Cl
2016-06-16 10:56:02	Delete					Internet Explorer - LsiBrowserHook Cl
2016-06-16 10:01:38	Change	0	1	RefCount		S-1-5-82-3006700770-424185619-174
2016-06-16 10:01:38	Change	0	1	Loaded		S-1-5-82-3006700770-424185619-174
2016-06-16 10:01:38	Change	#2016-06-15 20:32:14#	#2016-06-16 13:44:49#	LastWriteTime		S-1-5-82-3006700770-424185619-174
2016-06-16 10:01:35	Change	#2016-06-15 08:55:10#	#2016-06-16 09:44:54#	LastLogin		LSI\davidz
2016-06-16 10:01:34	Delete					Windows Malicious Software Removal
2016-06-16 10:01:33	Delete					Definition Update for Windows Defenc
2016-06-16 10:01:33	Delete					Cumulative Update for Windows 10 Ve
2016-06-16 10:01:33	Delete					Update for Windows 10 Version 1511
2016-06-16 10:01:33	Add					Windows Malicious Software Removal
2016-06-16 10:01:33	Add					Cumulative Update for Windows 10 Ve
2016-06-16 10:01:33	Add					Update for Windows 10 Version 1511
2016-06-16 10:00:36	Delete					Systems Management Agent (Lakeside
2016-06-16 10:00:36	Add					Systems Management Agent (Lakeside

Click here to roll back changes to the selected restore point

Roll Back the System to a Restore Point

After reviewing the related affected changed data, if you decide to roll back the system to a restore point:

1. Click to select the restore point on the graph.

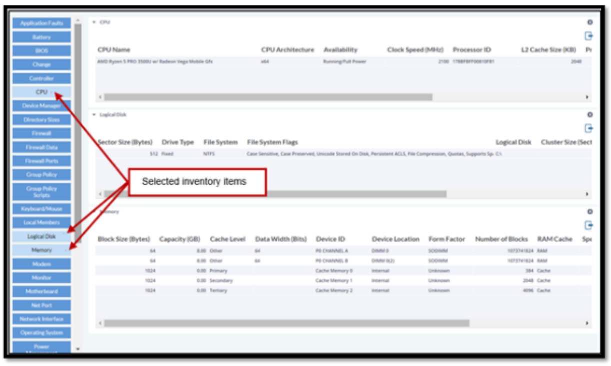


Time	Restore Point
2016-06-16 04:00:00	Windows Update
2016-06-13 04:00:00	Windows Update
2016-06-10 04:00:00	Windows Update

2. Click the ⟲ restore icon.
3. Using the resulting confirmation dialog box, click **Yes** if you are sure you want to restore to this point.
4. Using the resulting authorization dialog box, enter your Username and Password, and then click **OK**. If you have administrative privileges for the focus system, the system gets rebooted and rolled back to the selected restored point.

4.4.14 All Inventory Tool

This tool provides data for each of the system's existing inventory items in a tabular format. Clicking to select an inventory item displays the data associated with that item. You can click a column header to sort the table by that column's data.



CPU

CPU Name	CPU Architecture	Availability	Clock Speed (MHz)	Processor ID	L2 Cache Size (KB)	Pr
AMD Ryzen 5 PRO 3500U w/ Radeon Vega Mobile Gfx	x64	Running/Full Power	2100	178BFBFF00810F81	2048	

Logical Disk

Sector Size (Bytes)	Drive Type	File System	File System Flags	Logical Disk	Cluster Size (Sect
512	Fixed	NTFS	Case Sensitive, Case Preserved, Unicode Stored On Disk, Persistent ACLS, File Compression, Quotas, Supports Sp	C:\	

Memory

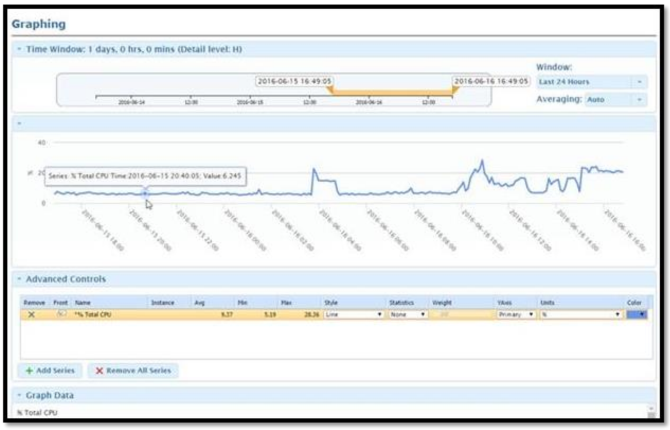
Block Size (Bytes)	Capacity (GB)	Cache Level	Data Width (Bits)	Device ID	Device Location	Form Factor	Number of Blocks	RAM Cache	Spe
64	8.00	Other	64	P0 CHANNEL A	DIMM 0	SODIMM	1073741824	RAM	
64	8.00	Other	64	P0 CHANNEL B	DIMM 0(2)	SODIMM	1073741824	RAM	
1024	0.00	Primary		Cache Memory 0	Internal	Unknown	384	Cache	
1024	0.00	Secondary		Cache Memory 1	Internal	Unknown	2048	Cache	
1024	0.00	Tertiary		Cache Memory 2	Internal	Unknown	4096	Cache	

4.4.15 Graphing

This tool generates graphs for selected system metrics and milestones over a specified time. Multiple graphs are overlaid, allowing you to easily view and compare related concerns.

The table below describes each of the tool's components. Click each link for detailed instructions for using each component.

Component	Description
Time Window	Allows you to set the window of time for the tool's data. Additionally, allows you to select the detail level and averaging settings for the graph data.
Graph	% Total CPU is the graph's default series of data points. You can control what displays in the graph by adding or deleting data set series. Clicking on a graph datapoint opens the Black Box tool, allowing you to review what was happening on the system at that point in time(e.g., which applications were active).
Advanced Controls	Once you have added a series to the graph, you can use these controls to determine how the data series or milestones display on the graph. For example, you can apply a statistical function to a data series, or you can change the data's units.
Add Series	Allows you to add additional data series or milestones to the graph.
Graph Data	Displays the data for each added series in a tabular format.



Graphing

Time Window: 1 days, 0 hrs, 0 mins (Detail level: H)

Window: Last 24 Hours

Averaging: Auto

Series: % Total CPU Time 2016-06-15 20:40:05; Value 6.245

Advanced Controls

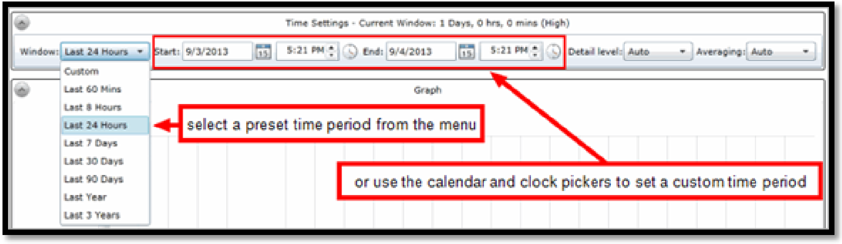
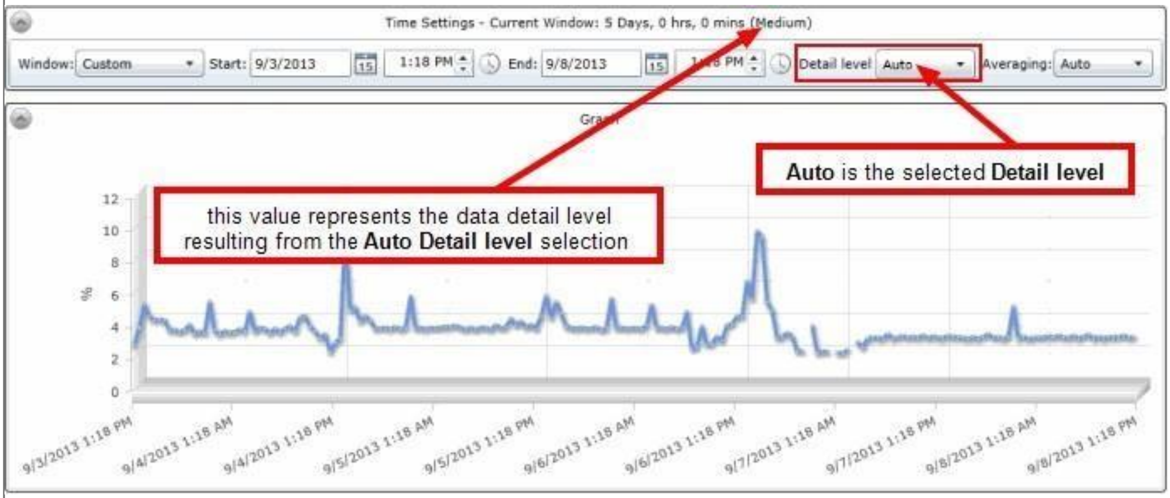
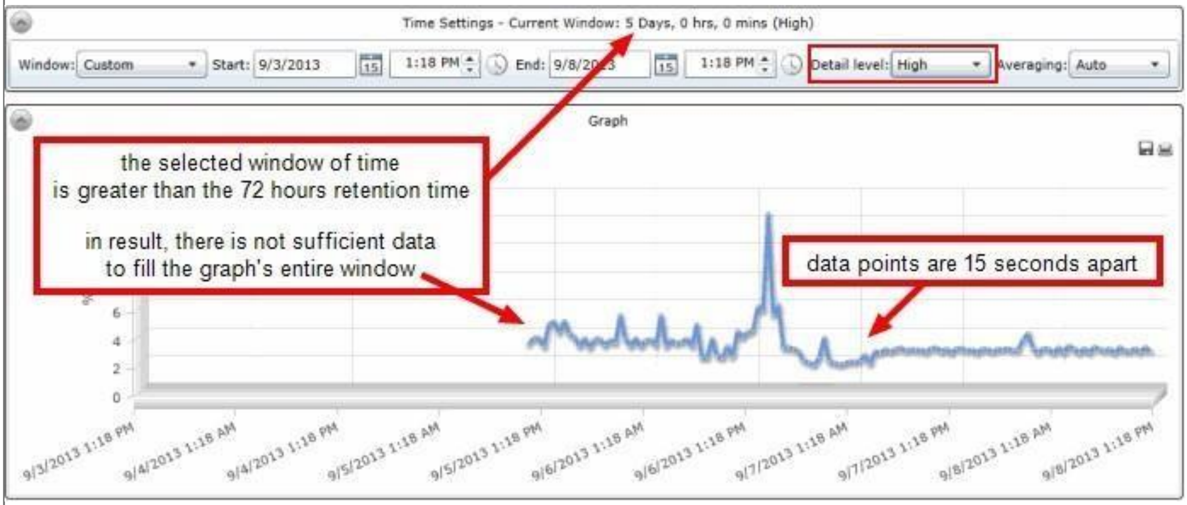
Remove	Front	Name	Instance	Avg	Min	Max	Style	Statistics	Weight	YAxis	Units	Color
✕		*% Total CPU		9.37	5.19	28.36	Line	None		Primary	%	

Graph Data

% Total CPU

Adjust the Time Settings

When using the Black Box Tool, you use the Time Settings control to set the window of timefor the graph. When using the Graphing Tool, you use the Time Settings control to set the window of time for the all of the tool's data.

Detail Level	Description
Auto	 Time Settings - Current Window: 1 Days, 0 hrs, 0 mins (High) Window: Last 24 Hours Start: 9/3/2013 5:21 PM End: 9/4/2013 5:21 PM Detail level: Auto Averaging: Auto Custom Last 60 Mins Last 8 Hours Last 24 Hours Last 7 Days Last 30 Days Last 90 Days Last Year Last 3 Years Graph select a preset time period from the menu or use the calendar and clock pickers to set a custom time period Displays the highest-level data available that provides sufficient data to fill the entire time window is used, and the selected window of time. For all other levels, the requested level of data detail is used.  Time Settings - Current Window: 5 Days, 0 hrs, 0 mins (Medium) Window: Custom Start: 9/3/2013 1:18 PM End: 9/8/2013 1:18 PM Detail level: Auto Averaging: Auto Graph % 12 10 8 6 4 2 0 9/3/2013 1:18 PM 9/4/2013 1:18 AM 9/4/2013 1:18 PM 9/5/2013 1:18 AM 9/5/2013 1:18 PM 9/6/2013 1:18 AM 9/6/2013 1:18 PM 9/7/2013 1:18 AM 9/7/2013 1:18 PM 9/8/2013 1:18 AM 9/8/2013 1:18 PM Auto is the selected **Detail level** this value represents the data detail level resulting from the **Auto Detail level** selection
High	Provides the finest data granularity; data points are collected every 15 seconds and are retained.  Time Settings - Current Window: 5 Days, 0 hrs, 0 mins (High) Window: Custom Start: 9/3/2013 1:18 PM End: 9/8/2013 1:18 PM Detail level: High Averaging: Auto Graph % 6 4 2 0 9/3/2013 1:18 PM 9/4/2013 1:18 AM 9/4/2013 1:18 PM 9/5/2013 1:18 AM 9/5/2013 1:18 PM 9/6/2013 1:18 AM 9/6/2013 1:18 PM 9/7/2013 1:18 AM 9/7/2013 1:18 PM 9/8/2013 1:18 AM 9/8/2013 1:18 PM the selected window of time is greater than the 72 hours retention time in result, there is not sufficient data to fill the graph's entire window data points are 15 seconds apart
Medium	Data points are collected every 10 minutes and are retained for 30 days.

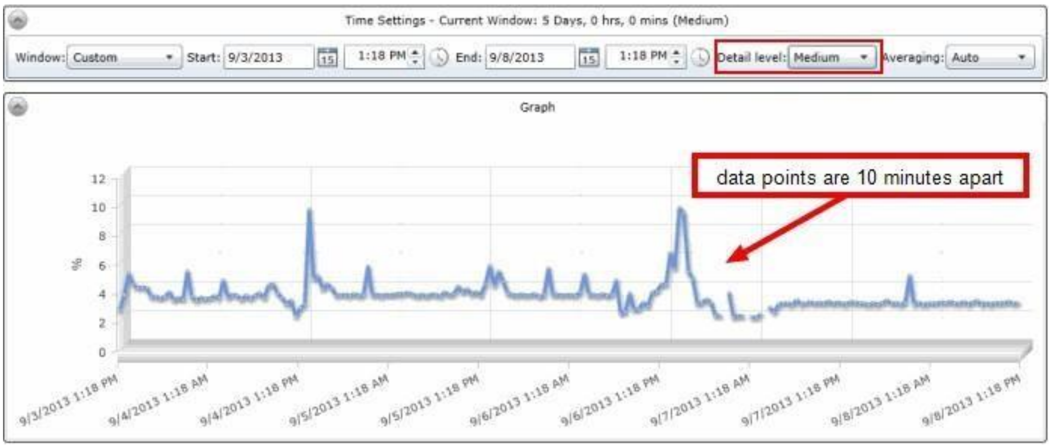
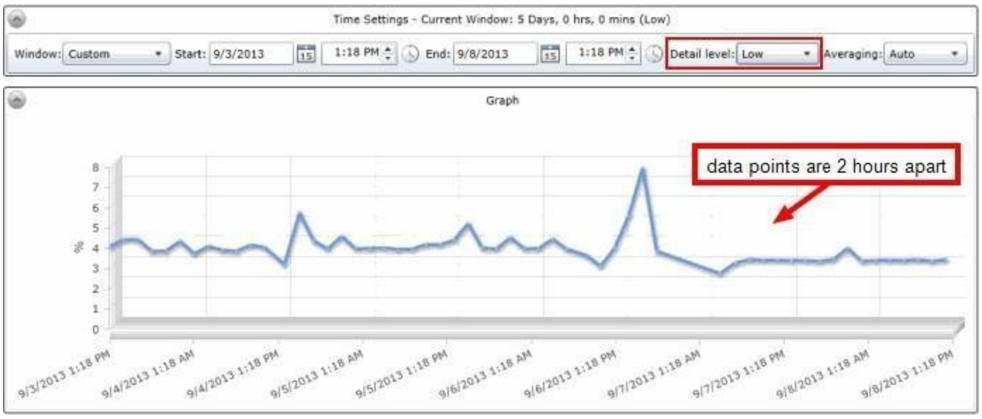
You can select one of the preset time periods, or you can use the date and time pickers to manually set the window's Start and End times. If the Start and End times are changed manually, the window size is set to

Custom. The time settings pane also allows you to select the Detail level and Averaging settings for the graph data.

Select the Detail Level

The Detail level selection allows you to control the data detail level being requested. The following table describes each detail level.

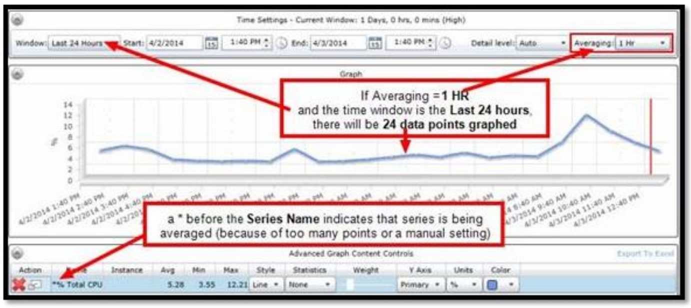
Although the selected Detail level is different in each of the example screen shots below, the selected window of time is identical.

Detail Level	Description
Medium	 Time Settings - Current Window: 5 Days, 0 hrs, 0 mins (Medium) Window: Custom Start: 9/3/2013 1:18 PM End: 9/8/2013 1:18 PM Detail level: Medium Averaging: Auto Graph data points are 10 minutes apart % 12 10 8 6 4 2 0 9/3/2013 1:18 PM 9/4/2013 1:18 AM 9/4/2013 1:18 PM 9/5/2013 1:18 AM 9/5/2013 1:18 PM 9/6/2013 1:18 AM 9/6/2013 1:18 PM 9/7/2013 1:18 AM 9/7/2013 1:18 PM 9/8/2013 1:18 AM 9/8/2013 1:18 PM
Low	Provides summarized data; data points are collected every 2 hours and are retained for 3 years  Time Settings - Current Window: 5 Days, 0 hrs, 0 mins (Low) Window: Custom Start: 9/3/2013 1:18 PM End: 9/8/2013 1:18 PM Detail level: Low Averaging: Auto Graph data points are 2 hours apart % 8 7 6 5 4 3 2 1 0 9/3/2013 1:18 PM 9/4/2013 1:18 AM 9/4/2013 1:18 PM 9/5/2013 1:18 AM 9/5/2013 1:18 PM 9/6/2013 1:18 AM 9/6/2013 1:18 PM 9/7/2013 1:18 AM 9/7/2013 1:18 PM 9/8/2013 1:18 AM 9/8/2013 1:18 PM

Select the Averaging Setting

The Averaging setting controls how the raw data points are treated before being graphed. If Auto is selected, the raw data points are graphed without being altered if there are not too many points to graph (high detail and/or long window time). The maximum number of points that can be graphed is 500. Above that, the chart averages the points so that they meet the 500-point maximum. If the setting is anything other than Auto, the data is averaged into periods as defined by the setting. For example, if the Averaging setting is 1 HR and the time window is the last 24 hours, there are 24 data points graphed. If the raw data is at a higher sample rate than 1 hour, the points occurring in each hour are averaged to get the value for that hour's data point.

Note: When a series is being averaged (because of too many points or a manual setting), a * proceeds the series name.



Time Settings - Current Window: 1 Days, 0 hrs, 0 mins (High)

Window: Last 24 Hours | Start: 4/2/2014 | 1:40 PM | End: 4/3/2014 | 1:40 PM | Detail level: Auto | Averaging: 1 Hr

If Averaging =1 HR
and the time window is the **Last 24 hours**,
there will be **24 data points graphed**

a * before the **Series Name** indicates that series is being
averaged (because of too many points or a manual setting)

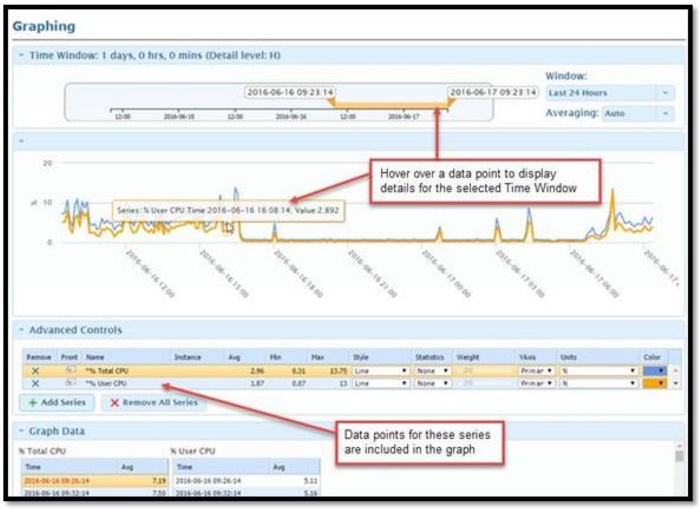
Advanced Graph Content Controls

Action	Name	Instance	Avg	Min	Max	Style	Statistics	Weight	Y Axis	Units	Color
	*% Total CPU		5.28	3.55	12.21	Line	None		Primary	%	

Graph

% Total CPU is the graph's default series of data points. You can control what displays on thegraph by adding or deleting data set series using the Advanced Controls.

Hovering over the graph displays the details for any series' data points for the specified date and time.



Graphing

Time Window: 1 days, 0 hrs, 0 mins (Detail level: H)

Window: Last 24 Hours

Averaging: Auto

Hover over a data point to display details for the selected Time Window

Series: % User CPU Time 2016-06-16 16:08:14, Value 2.892

Advanced Controls

Remove	Front	Name	Instance	Avg	Min	Max	Style	Statistics	Weight	YAxis	Units	Color
✕		*% Total CPU		2.96	0.31	13.75	Line	None	20	Primar	%	
✕		*% User CPU		1.87	0.07	13	Line	None	20	Primar	%	

Data points for these series are included in the graph

Graph Data

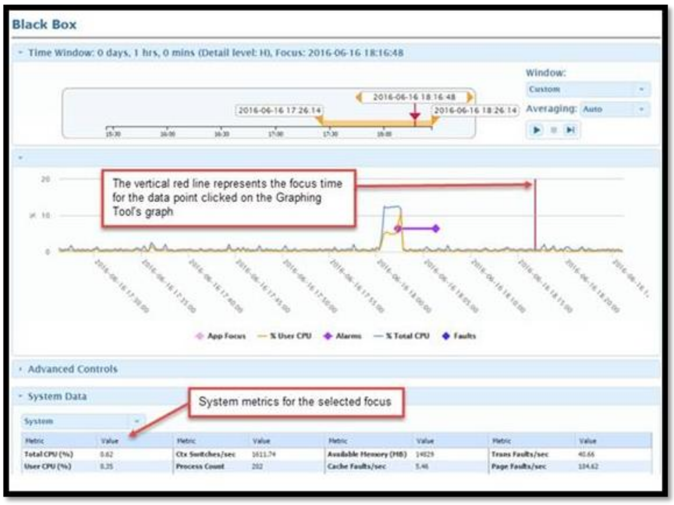
% Total CPU

Time	Avg
2016-06-16 09:26:14	7.19
2016-06-16 09:32:14	7.50

% User CPU

Time	Avg
2016-06-16 09:26:14	5.11
2016-06-16 09:32:14	5.16

Clicking any data point in a series open the Black Box tool (as shown below), allowing you toreview what was happening on the system at that point in time (e.g., which applications were active).



Black Box

Time Window: 0 days, 1 hrs, 0 mins (Detail level: H), Focus: 2016-06-16 18:16:48

Window: Custom

Averaging: Auto

The vertical red line represents the focus time for the data point clicked on the Graphing Tool's graph

Advanced Controls

System Data

System metrics for the selected focus

System

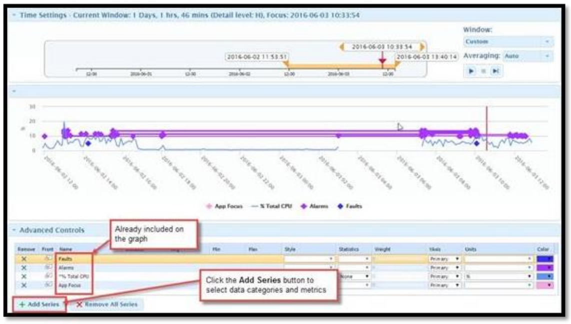
Metric	Value	Metric	Value	Metric	Value	Metric	Value
Total CPU (%)	0.62	Ctx Switches/sec	1611.74	Available Memory (MB)	14829	Trans Faults/sec	40.66
User CPU (%)	0.25	Process Count	202	Cache Faults/sec	5.46	Page Faults/sec	104.62

Add a Data Series to the Graph

From select data grid categories, you can choose metrics to add to the graph as a data series. Any series you add will persist throughout your current Device Lookup session. Once you have added a data series to the graph, you can use the Advanced Graph ContentControls for functionality such as changing the series' graphical style or units.

To add a data series to the graph:

1. From the Advanced Controls pane, click the **Add Series** Button.
2. From the **Add Series** dialog, click to select the metric(s) you wish to add tothe graph as a data

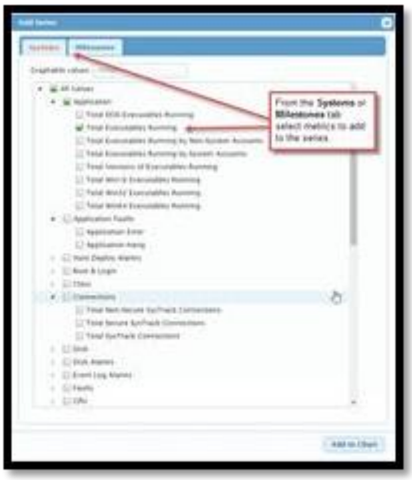


Already included on the graph

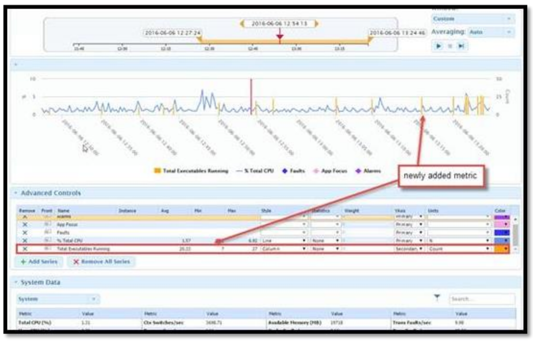
Click the **Add Series** button to select data categories and metrics

series.

The selected metric is added to the Advanced Controls table and to the graph as a data series.



From the **Systems** or **Milestones** tab select metric(s) to add to the series



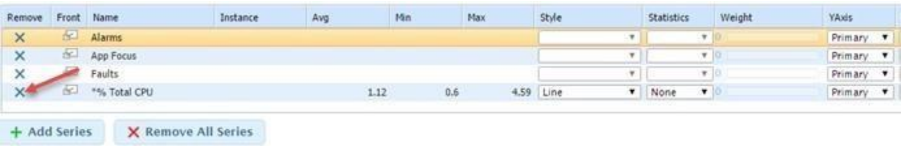
newly added metric

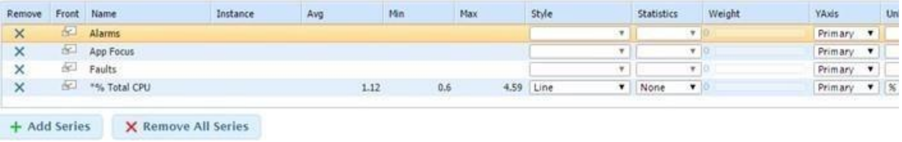
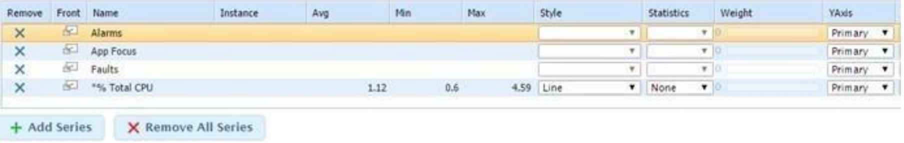
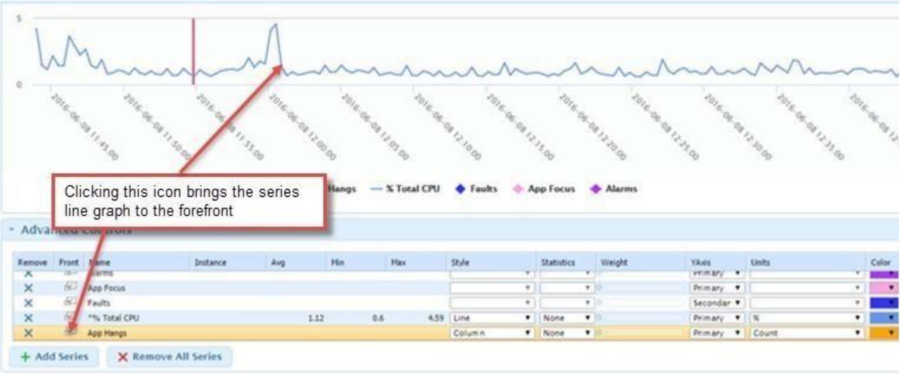
3. To remove a series from the graph, click the **X** to the left of the metric in theAdvance Controls table that you wish to remove.
4. If you wish to remove all the series listed in the Advanced Controls table, clickthe **Remove All Series** button.

You can also add certain metrics from the System Data grid to the graph.

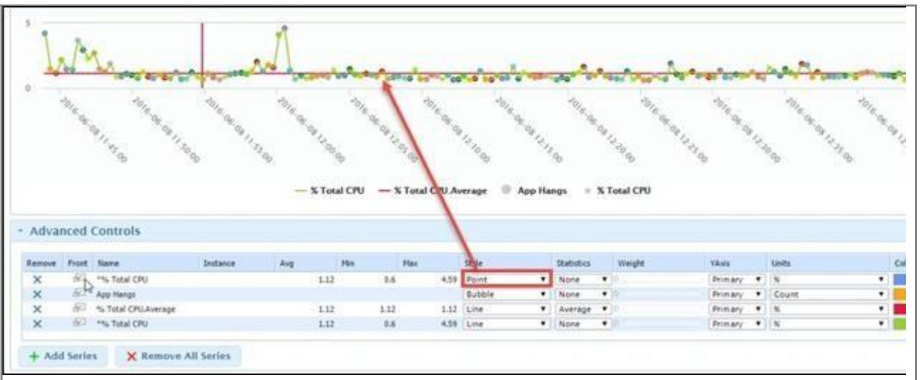
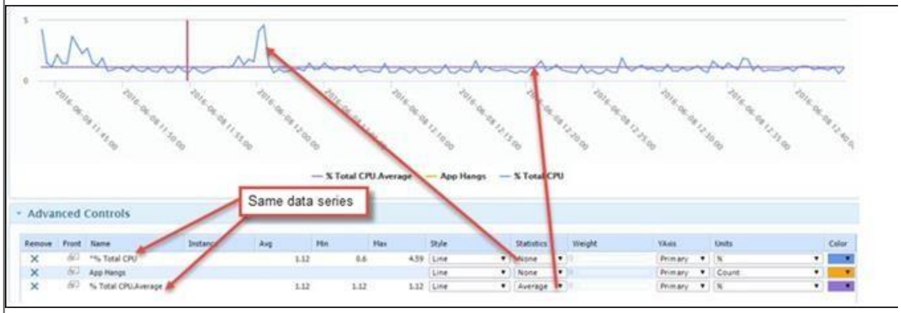
Advanced Graph Content Controls

The following table describes each of the available Advanced Graph Content Controls:

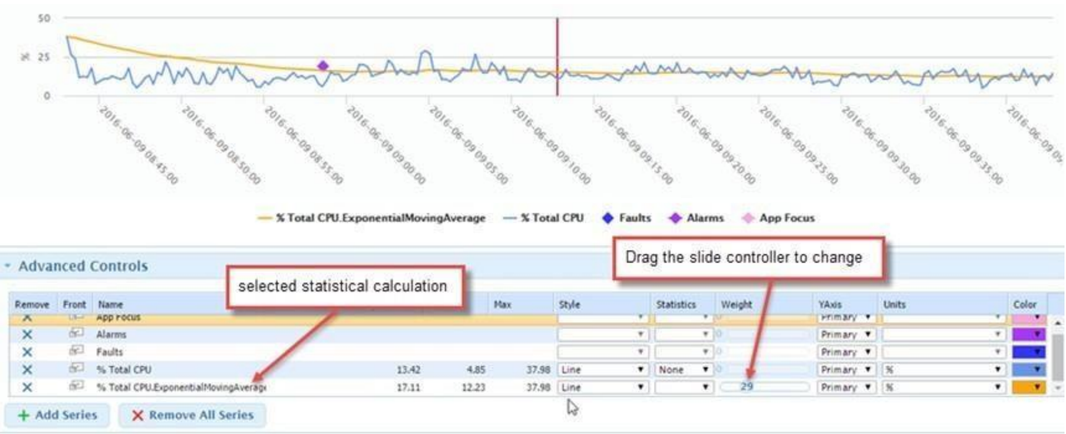
<table>
<tr><th>Control</th><th>Description</th></tr>
<tr><td>✕</td><td>Clicking this control icon will remove a data series from the graph.

<table><tr><th>Remove</th><th>Front</th><th>Name</th><th>Instance</th><th>Avg</th><th>Min</th><th>Max</th><th>Style</th><th>Statistics</th><th>Weight</th><th>YAxis</th></tr><tr><td>✕</td><td></td><td>Alarms</td><td></td><td></td><td></td><td></td><td>▾</td><td>▾</td><td>0</td><td>Primary ▾</td></tr><tr><td>✕</td><td></td><td>App Focus</td><td></td><td></td><td></td><td></td><td>▾</td><td>▾</td><td>0</td><td>Primary ▾</td></tr><tr><td>✕</td><td></td><td>Faults</td><td></td><td></td><td></td><td></td><td>▾</td><td>▾</td><td>0</td><td>Primary ▾</td></tr><tr><td>✕</td><td></td><td>*% Total CPU</td><td></td><td>1.12</td><td>0.6</td><td>4.59</td><td>Line ▾</td><td>None ▾</td><td>0</td><td>Primary ▾</td></tr></table> </td></tr>
</table>

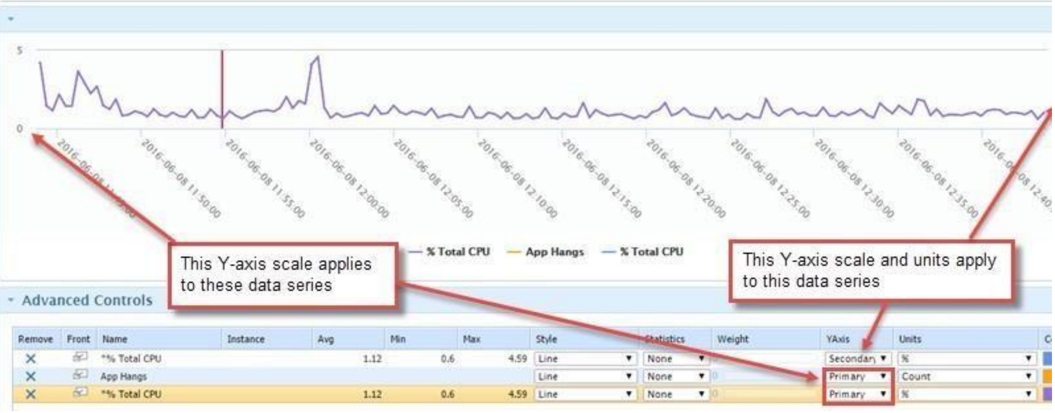
✕ Remove All Se	Clicking this control icon removes all the data series from thegraph.  Remove · Front · Name · Instance · Avg · Min · Max · Style · Statistics · Weight · YAxis · Un ✕ · Alarms · Primary ✕ · App Focus · Primary ✕ · Faults · Primary ✕ · *% Total CPU · 1.12 · 0.6 · 4.59 · Line · None · Primary · % + Add Series · ✕ Remove All Series
+ Add Series	 Remove · Front · Name · Instance · Avg · Min · Max · Style · Statistics · Weight · YAxis ✕ · Alarms · Primary ✕ · App Focus · Primary ✕ · Faults · Primary ✕ · *% Total CPU · 1.12 · 0.6 · 4.59 · Line · None · Primary + Add Series · ✕ Remove All Series
⧉	Clicking this control icon moves the series to the foreground of the graph. This control is especially useful if there are series with data points overlaying each other on the graph.  5 0 2016-06-08 11:45:00 2016-06-08 11:50:00 2016-06-08 11:55:00 2016-06-08 12:00:00 2016-06-08 12:05:00 2016-06-08 12:10:00 2016-06-08 12:15:00 2016-06-08 12:20:00 2016-06-08 12:25:00 2016-06-08 12:30:00 2016-06-08 12:35:00 Hangs % Total CPU Faults App Focus Alarms Clicking this icon brings the series line graph to the forefront Advanced Controls Remove · Front · Name · Instance · Avg · Min · Max · Style · Statistics · Weight · YAxis · Units · Color ✕ · Alarms · Primary ✕ · App Focus · Primary ✕ · Faults · Secondar ✕ · *% Total CPU · 1.12 · 0.6 · 4.59 · Line · None · Primary · % ✕ · App Hangs · Column · None · Primary · Count + Add Series · ✕ Remove All Series

Style	Allows you to change how a series is presented on the graph. For example, by changing the Style selection from **Line** to **Point**, data points displayed as a line are changed to individual points. When multiple series are graphed, the list of **Style** options is filtered to those compatible with the type selected for the first series.

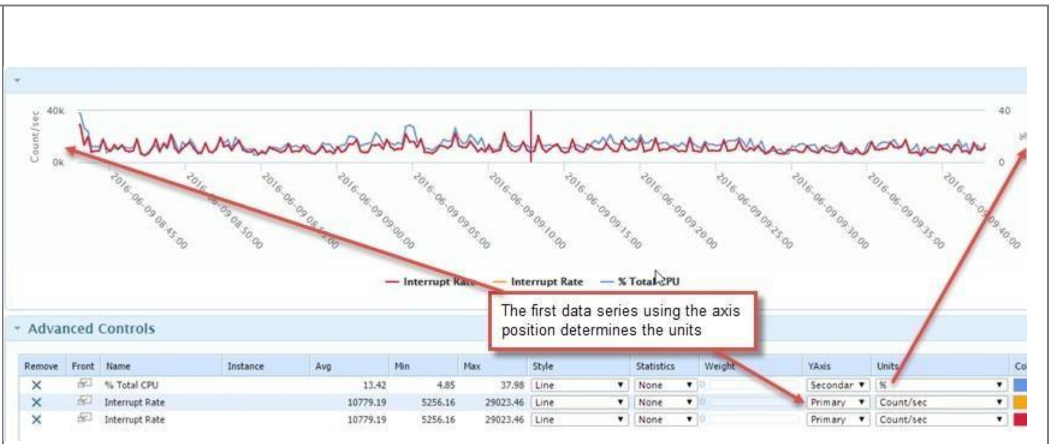
<table>
<tr><td></td><td>
<table>
<tr><th>Remove</th><th>Front</th><th>Name</th><th>Instance</th><th>Avg</th><th>Min</th><th>Max</th><th>Style</th><th>Statistics</th><th>Weight</th><th>YAxis</th><th>Units</th><th>Col</th></tr>
<tr><td>✕</td><td></td><td>**% Total CPU</td><td></td><td>1.12</td><td>0.6</td><td>4.59</td><td>Point</td><td>None</td><td>0</td><td>Primary</td><td>%</td><td>🟦</td></tr>
<tr><td>✕</td><td></td><td>App Hangs</td><td></td><td></td><td></td><td></td><td>Bubble</td><td>None</td><td>0</td><td>Primary</td><td>Count</td><td>🟧</td></tr>
<tr><td>✕</td><td></td><td>% Total CPU.Average</td><td></td><td>1.12</td><td>1.12</td><td>1.12</td><td>Line</td><td>Average</td><td>0</td><td>Primary</td><td>%</td><td>🟥</td></tr>
<tr><td>✕</td><td></td><td>**% Total CPU</td><td></td><td>1.12</td><td>0.6</td><td>4.59</td><td>Line</td><td>None</td><td>0</td><td>Primary</td><td>%</td><td>🟩</td></tr>
</table></td></tr>
<tr><td>Statistics</td><td>If you select a value other than None, a copy of the data set will be made and added to the graph with the chosen statistical function applied to the copy.

<table>
<tr><th>Remove</th><th>Front</th><th>Name</th><th>Instance</th><th>Avg</th><th>Min</th><th>Max</th><th>Style</th><th>Statistics</th><th>Weight</th><th>YAxis</th><th>Units</th><th>Color</th></tr>
<tr><td>✕</td><td></td><td>**% Total CPU</td><td></td><td>1.12</td><td>0.6</td><td>4.59</td><td>Line</td><td>None</td><td>0</td><td>Primary</td><td>%</td><td>🟦</td></tr>
<tr><td>✕</td><td></td><td>App Hangs</td><td></td><td></td><td></td><td></td><td>Line</td><td>None</td><td>0</td><td>Primary</td><td>Count</td><td>🟧</td></tr>
<tr><td>✕</td><td></td><td>% Total CPU.Average</td><td></td><td>1.12</td><td>1.12</td><td>1.12</td><td>Line</td><td>Average</td><td>0</td><td>Primary</td><td>%</td><td>🟪</td></tr>
</table></td></tr>
<tr><td>Weight</td><td>The weight value is a value used as a factor select statistical calculations. It can be applied to the following statistical calculations: <b>Bollinger, Exponential Moving Average; Modified Moving Average; Simple Moving Average; Weighted Moving Average; Momentum; Momentum Division;</b> and <b>Power</b>. You use the <b>Weight</b> slider to select the weight factor - ranging from 1 - 100%.The value that it modifies varies with the statistical calculation selected. For most calculations, it scales the count of points in the data set to be graphed and uses the scaled value as the factor in the
statical calculation.</td></tr>
</table>

Control	**Description**

<table>
<tr>
<td></td>
<td>


selected statistical calculation
Drag the slide controller to change
<table>
<tr><th>Remove</th><th>Front</th><th>Name</th><th></th><th></th><th>Max</th><th>Style</th><th>Statistics</th><th>Weight</th><th>YAxis</th><th>Units</th><th>Color</th></tr>
<tr><td>✕</td><td></td><td>App Focus</td><td></td><td></td><td></td><td></td><td></td><td></td><td>Primary</td><td></td><td></td></tr>
<tr><td>✕</td><td></td><td>Alarms</td><td></td><td></td><td></td><td></td><td></td><td>0</td><td>Primary</td><td></td><td></td></tr>
<tr><td>✕</td><td></td><td>Faults</td><td></td><td></td><td></td><td></td><td></td><td>0</td><td>Primary</td><td></td><td></td></tr>
<tr><td>✕</td><td></td><td>% Total CPU</td><td>13.42</td><td>4.85</td><td>37.98</td><td>Line</td><td>None</td><td>0</td><td>Primary</td><td>%</td><td></td></tr>
<tr><td>✕</td><td></td><td>% Total CPU.ExponentialMovingAverage</td><td>17.11</td><td>12.23</td><td>37.98</td><td>Line</td><td></td><td>29</td><td>Primary</td><td>%</td><td></td></tr>
</table>
</td>
</tr>
<tr>
<td>Y Axis</td>
<td>
Controls which axis position the series Y data is charted on. When <b>Primary</b> is sele cted, the scale on the <i>left</i> side of the chart applies to the series.
When <b>Secondary</b> is selected, the scale on the <i>right</i> side of the chart applies to the series.


This Y-axis scale applies to these data series
This Y-axis scale and units apply to this data series
<table>
<tr><th>Remove</th><th>Front</th><th>Name</th><th>Instance</th><th>Avg</th><th>Min</th><th>Max</th><th>Style</th><th>Statistics</th><th>Weight</th><th>YAxis</th><th>Units</th></tr>
<tr><td>✕</td><td></td><td>*% Total CPU</td><td></td><td>1.12</td><td>0.6</td><td>4.59</td><td>Line</td><td>None</td><td></td><td>Secondary</td><td>%</td></tr>
<tr><td>✕</td><td></td><td>App Hangs</td><td></td><td></td><td></td><td></td><td>Line</td><td>None</td><td>0</td><td>Primary</td><td>Count</td></tr>
<tr><td>✕</td><td></td><td>*% Total CPU</td><td></td><td>1.12</td><td>0.6</td><td>4.59</td><td>Line</td><td>None</td><td>0</td><td>Primary</td><td>%</td></tr>
</table>
</td>
</tr>
<tr>
<td>Units</td>
<td>The units being used for the data series. Depending on the data, you may beable to select different units for the series if the initial units can be easily converted. When more than one series shares a Y axis position (Primary or Secondary), the first series added to that position will determine which units are used, but the scale will encompass the values from all series.</td>
</tr>
</table>

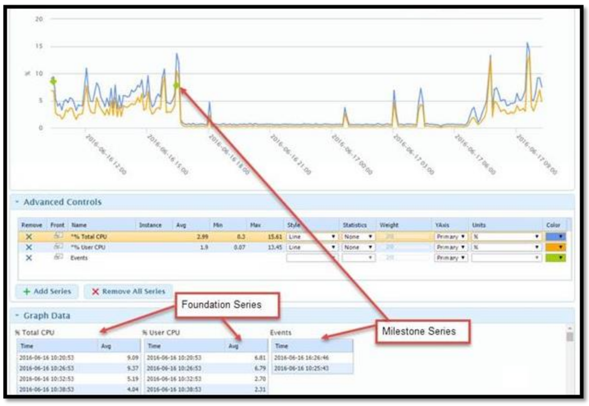
	
Color	The color used to render the series data on the graph. This column can act asa color key for the graph's series.

The first data series using the axis position determines the units

Remove	Front	Name	Instance	Avg	Min	Max	Style	Statistics	Weight	YAxis	Units	Co
✕		% Total CPU		13.42	4.85	37.98	Line	None	0	Secondar	%	🟦
✕		Interrupt Rate		10779.19	5256.16	29023.46	Line	None	0	Primary	Count/sec	🟧
✕		Interrupt Rate		10779.19	5256.16	29023.46	Line	None	0	Primary	Count/sec	🟥

View the Graph Data

This Graphing Tool component displays the data for each added series in a tabular format.



Remove	Front	Name	Instance	Avg	Min	Max	Style	Statistics	Weight	YAxis	Units	Color
✕		*% Total CPU		2.99	0.3	15.61	Line	None		Primary	%	🟦
✕		*% User CPU		1.9	0.07	13.45	Line	None		Primary	%	🟧
✕		Events								Primary		🟩

Foundation Series

Milestone Series

% Total CPU

Time	Avg
2016-06-16 10:20:53	9.09
2016-06-16 10:26:53	9.37
2016-06-16 10:32:53	5.19
2016-06-16 10:38:53	4.04

% User CPU

Time	Avg
2016-06-16 10:20:53	6.81
2016-06-16 10:26:53	6.79
2016-06-16 10:32:53	2.70
2016-06-16 10:38:53	2.31

Events

Time
2016-06-16 16:26:46
2016-06-16 10:25:43

For Foundation series added to the graph, there is one data row for each data point. For Milestone series added to the graph, there is one data row for each milestone charted.

4.4.16 Comparative Analytics

This tool allows you to compare selected metrics collected from the focus system metrics to the metrics of one or more groups of systems.

You have the option of displaying the threshold values for each group's metrics (threshold values are displayed within parentheses). Threshold values are based on average consumption; they are calculated by averaging the values collected from all systems in the group and then adding the standard deviation.

Yellow highlighting is used to indicate potential issues with the focus system's metric values.For some metrics, such as **Total I/O Operations**, there could potentially be an issue if a system has a metric value above one or more of the selected group's threshold values. In this case yellow highlighting is applied to the Metric name and to the groups' values that thefocus system's metric value falls above.

For other metrics, such as **Memory Capacity**, there could potentially be an issue if a system has a metric value below one or more of the selected group's threshold values. In this case yellow highlighting is applied to the Metric name and to the groups' values that the focussystem's metric value falls below.

Before deciding if there is an issue, you need to consider the metric value's context. For example, if a system has a **User Files** value that is above a selected group's threshold value, but the focus system has a much larger than average amount of storage space available, there is probably not an issue.

To use the tool’s features:

Any selections you make (metrics, group, and threshold display state) persists in future Device Lookup sessions.

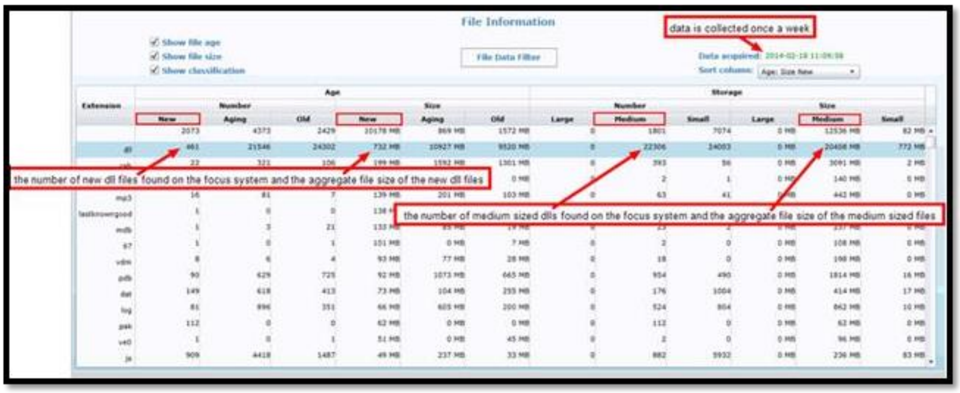
1. To determine which metrics are included in the table, select the Metrics tab, and then check or uncheck the boxes of the metrics you wish to include or exclude.
2. To select the group or groups you want to include in the comparison, select the Groups tab, and then check, or uncheck the boxes of the groups you wish to include or exclude.
3. Check the Show Threshold box to add threshold values to the selected groups' metrics. The threshold values be displayed in parentheses.

File Information

This tool groups all files found on the focus system by file extension, and then provides file age and file size data for each extension. This data is collected once a week. The tool provides options that allow you to customize how the data is displayed.

In the example shown below, we have highlighted file data for all files on the system with a dll extension. This data is first broken down by Age and by Size. The Age of a file is either classified as New, Aging, or Old. The Size of a file is classified as Small, Medium, or Large. The number of files with the extension and the aggregate size of the files are provided for each Age and Size classification.

In the example below, there are a total of 461 **New** files with dll extensions and their aggregate file size is 732 MB, and there are 22306 Medium sized files and their aggregate file size is 20408 MB.



File Information

☑ Show file age
☑ Show file size
☑ Show classification

File Data Filter

data is collected once a week

Data acquired: 2014-02-18 11:09:58
Sort column: Age: Size New

Extension	Age						Storage					
	Number			Size			Number			Size		
	New	Aging	Old	New	Aging	Old	Large	Medium	Small	Large	Medium	Small
	2073	4373	2429	10178 MB	869 MB	1572 MB	0	1801	7074	0 MB	12536 MB	82 MB
dll	461	21546	24302	732 MB	10927 MB	9520 MB	0	22306	24003	0 MB	20408 MB	772 MB
[illegible]	22	321	106	199 MB	1592 MB	1301 MB	0	393	56	0 MB	3091 MB	2 MB
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	0 MB	[illegible]	2	1	0 MB	140 MB	0 MB
mp3	16	81	7	139 MB	201 MB	103 MB	0	63	41	0 MB	442 MB	0 MB
lastknowngood	1	0	0	138 MB	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
mdb	1	3	21	133 MB	[illegible]	[illegible]	[illegible]	23	2	[illegible]	237 MB	[illegible]
67	1	0	1	101 MB	0 MB	7 MB	0	2	0	0 MB	108 MB	0 MB
vdm	8	6	4	93 MB	77 MB	28 MB	0	18	0	0 MB	198 MB	0 MB
pdb	90	629	725	92 MB	1073 MB	665 MB	0	954	490	0 MB	1814 MB	16 MB
dat	149	618	413	73 MB	104 MB	255 MB	0	176	1004	0 MB	414 MB	17 MB
log	81	896	351	66 MB	605 MB	200 MB	0	524	804	0 MB	862 MB	10 MB
pak	112	0	0	62 MB	0 MB	0 MB	0	112	0	0 MB	62 MB	0 MB
v40	1	0	1	51 MB	0 MB	45 MB	0	2	0	0 MB	96 MB	0 MB
js	909	4418	1487	49 MB	237 MB	33 MB	0	882	5932	0 MB	236 MB	83 MB

the number of new dll files found on the focus system and the aggregate file size of the new dll files

the number of medium sized dlls found on the focus system and the aggregate file size of the medium sized files

The following tables define the default ranges of the Age and Size classifications. You can change the default ranges via the Deployment Tool.

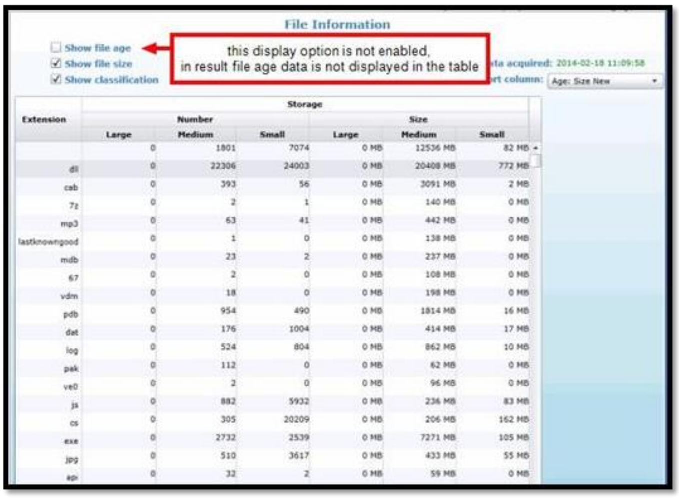
Age (at last access time)		
New	**Aging**	**Old**
newer than 30 days	between 30 days and 1 year	older than 1 year

Size

Small	Medium	Large
less than 100 KB (100,000 bytes)	between 100 KB and 1GB (100,000 and 1,000,000,000 bytes)	greater than 1 GB (1,000,000,000 bytes)

To use the File Information tool display options:

Use the **Show** check boxes to customize the table to only **Show file age data** or toonly **Show file size data**. In the example below, only file size data is displayed.



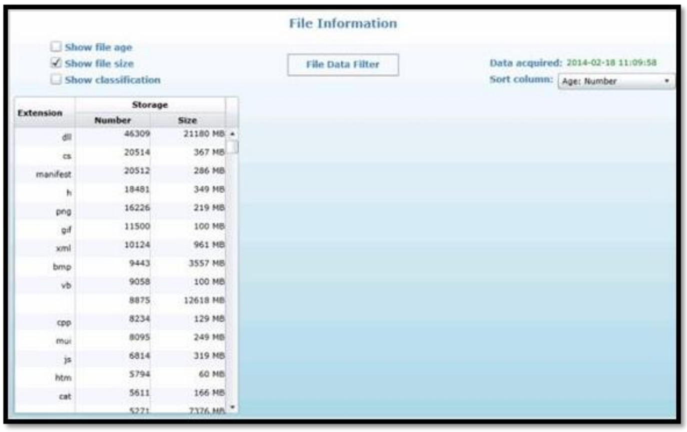
File Information

□ Show file age
☑ Show file size
☑ Show classification

this display option is not enabled,
in result file age data is not displayed in the table

ta acquired: 2014-02-18 11:09:58
rt column: Age: Size New

Extension	Storage					
	Number			Size		
	Large	Medium	Small	Large	Medium	Small
	0	1801	7074	0 MB	12536 MB	82 MB
dll	0	22306	24003	0 MB	20408 MB	772 MB
cab	0	393	56	0 MB	3091 MB	2 MB
7z	0	2	1	0 MB	140 MB	0 MB
mp3	0	63	41	0 MB	442 MB	0 MB
lastknowngood	0	1	0	0 MB	138 MB	0 MB
mdb	0	23	2	0 MB	237 MB	0 MB
67	0	2	0	0 MB	108 MB	0 MB
vdm	0	18	0	0 MB	198 MB	0 MB
pdb	0	954	490	0 MB	1814 MB	16 MB
dat	0	176	1004	0 MB	414 MB	17 MB
log	0	524	804	0 MB	862 MB	10 MB
pak	0	112	0	0 MB	62 MB	0 MB
ve0	0	2	0	0 MB	96 MB	0 MB
js	0	882	5932	0 MB	236 MB	83 MB
cs	0	305	20209	0 MB	206 MB	162 MB
exe	0	2732	2539	0 MB	7271 MB	105 MB
jpg	0	510	3617	0 MB	433 MB	55 MB
api	0	32	2	0 MB	59 MB	0 MB



File Information

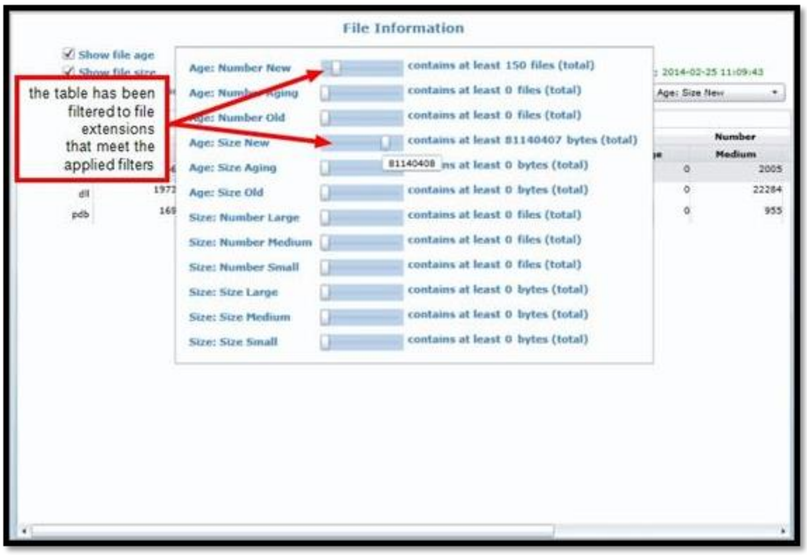
□ Show file age
☑ Show file size
□ Show classification

File Data Filter

Data acquired: 2014-02-18 11:09:58
Sort column: Age: Number

Extension	Storage	
	Number	Size
dll	46309	21180 MB
cs	20514	367 MB
manifest	20512	286 MB
h	18481	349 MB
png	16226	219 MB
gif	11500	100 MB
xml	10124	961 MB
bmp	9443	3557 MB
vb	9058	100 MB
	8875	12618 MB
cpp	8234	129 MB
mui	8095	249 MB
js	6814	319 MB
htm	5794	60 MB
cat	5611	166 MB
	5271	7376 MB

You can also remove the individual classification values and instead display one total valueby disabling the **Show classification** option. In the example shown below, in addition to displaying only file size data, we have opted to not display the classifications. In result, the **Number** column displays the sum of the number of large, medium, and small files; andthe **Size** column displays the sum of the file sizes of the large, medium, and small files.



File Information

☑ Show file age

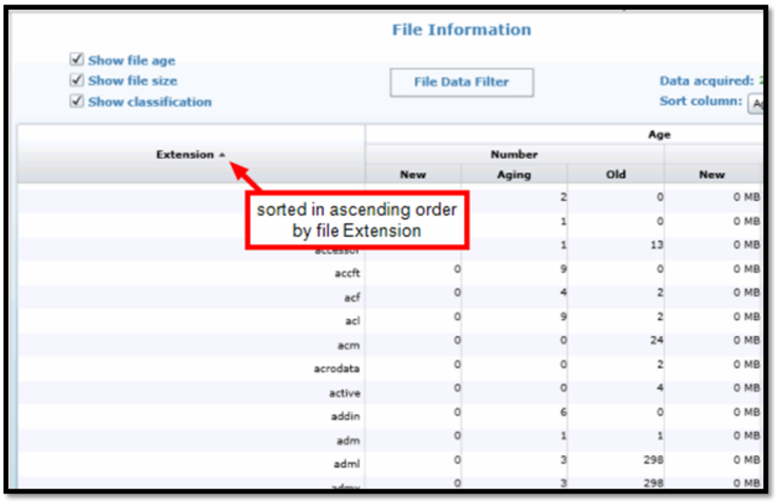
☑ Show file size

the table has been filtered to file extensions that meet the applied filters

Age: Number New — contains at least 150 files (total)
Age: Number Aging — contains at least 0 files (total)
Age: Number Old — contains at least 0 files (total)
Age: Size New — contains at least 81140407 bytes (total)
Age: Size Aging — 81140408 ns at least 0 bytes (total)
Age: Size Old — contains at least 0 bytes (total)
Size: Number Large — contains at least 0 files (total)
Size: Number Medium — contains at least 0 files (total)
Size: Number Small — contains at least 0 files (total)
Size: Size Large — contains at least 0 bytes (total)
Size: Size Medium — contains at least 0 bytes (total)
Size: Size Small — contains at least 0 bytes (total)

Moving your cursor over File Data Filter displays the available options for filtering column data. Use the slide controls to filter the Extensions included in the table by a specified minimum total number of files or minimum total number of bytes. The table filters dynamically as you move the slide controls. In the example shown below, we have filtered the table to only display data for file extensions that have at least 202 files categorized as new and contain at least 100000000 bytes (total).

You can sort the table data by file **Extension** or by a selected **Age** or **Size** column.



File Information

☑ Show file age

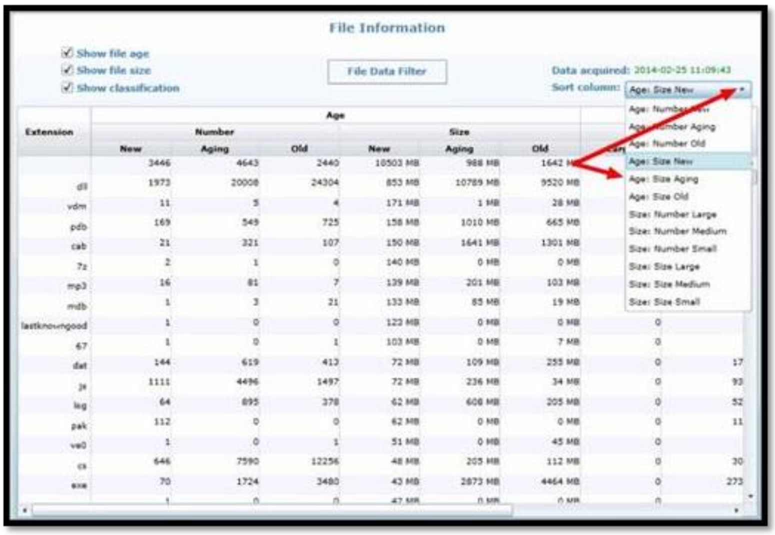
☑ Show file size

☑ Show classification

sorted in ascending order by file Extension

	Age			
	Number			
Extension ▲	New	Aging	Old	New
		2	0	0 MB
		1	0	0 MB
accessor		1	13	0 MB
accft	0	9	0	0 MB
acf	0	4	2	0 MB
acl	0	9	2	0 MB
acm	0	0	24	0 MB
acrodata	0	0	2	0 MB
active	0	0	4	0 MB
addin	0	6	0	0 MB
adm	0	1	1	0 MB
adml	0	3	298	0 MB
admx	0	3	298	0 MB

To sort the data by file **Extension**, click the **Extension** column header. The direction of the arrow indicates whether the column is sorted in ascending or descending order.


File Information

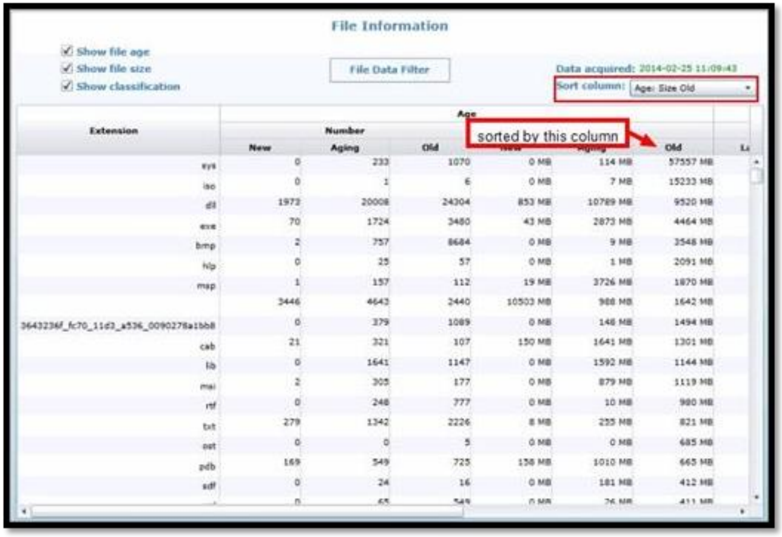
☑ Show file age
☑ Show file size
☑ Show classification

Data acquired: 2014-02-25 11:09:43
Sort column: Age: Size New

Extension	Age							
	Number			Size				
	New	Aging	Old	New	Aging	Old		
	3446	4643	2440	10503 MB	988 MB	1642 MB		
dll	1973	20008	24304	853 MB	10789 MB	9520 MB		
vdm	11	5	4	171 MB	1 MB	28 MB		
pdb	169	549	725	158 MB	1010 MB	665 MB		
cab	21	321	107	150 MB	1641 MB	1301 MB		
7z	2	1	0	140 MB	0 MB	0 MB		
mp3	16	81	7	139 MB	201 MB	103 MB		
mdb	1	3	21	133 MB	85 MB	19 MB		
lastknowngood	1	0	0	123 MB	0 MB	0 MB	0	
67	1	0	1	103 MB	0 MB	7 MB	0	
dat	144	619	413	72 MB	109 MB	255 MB	0	17
js	1111	4496	1497	72 MB	236 MB	34 MB	0	93
log	64	895	378	62 MB	608 MB	205 MB	0	52
pak	112	0	0	62 MB	0 MB	0 MB	0	11
ve0	1	0	1	51 MB	0 MB	45 MB	0	
cs	646	7590	12256	48 MB	205 MB	112 MB	0	30
exe	70	1724	3480	43 MB	2873 MB	4464 MB	0	273
	1	0	0	47 MB	0 MB	0 MB	0	

To sort the table by the data in an Age or Size column, click the Sort column drop-down arrow and select a column from the resulting menu.

In the example shown below, the table is sorted by the data in the Age: Size Old column.


File Information

☑ Show file age
☑ Show file size
☑ Show classification

Data acquired: 2014-02-25 11:09:43
Sort column: Age: Size Old

Extension	Age					
	Number					
	New	Aging	Old	New	Aging	Old
sys	0	233	1070	0 MB	114 MB	57557 MB
iso	0	1	6	0 MB	7 MB	15233 MB
dll	1973	20008	24304	853 MB	10789 MB	9520 MB
exe	70	1724	3480	43 MB	2873 MB	4464 MB
bmp	2	757	8684	0 MB	9 MB	3548 MB
hlp	0	25	57	0 MB	1 MB	2091 MB
map	1	157	112	19 MB	3726 MB	1870 MB
	3446	4643	2440	10503 MB	988 MB	1642 MB
3643236f_fc70_11d3_a536_0090278a1bb8	0	379	1089	0 MB	148 MB	1494 MB
cab	21	321	107	150 MB	1641 MB	1301 MB
lib	0	1641	1147	0 MB	1592 MB	1144 MB
msi	2	305	177	0 MB	879 MB	1119 MB
rtf	0	248	777	0 MB	10 MB	980 MB
txt	279	1342	2226	8 MB	255 MB	821 MB
ost	0	0	5	0 MB	0 MB	685 MB
pdb	169	549	725	158 MB	1010 MB	665 MB
sdf	0	24	16	0 MB	181 MB	412 MB
	0	65	549	0 MB	26 MB	411 MB

4.4.17 Power Schedule

The Power Schedule tool displays Power Saving Hours (week), Power/Cooling Costs, Estimated Cost (month) and Savings (month) for devices. The Power Schedule grid displays power consumption based on User Activity, System Activity and Effective categories.

4.4.18 Tools

Tools allows you to run automations on a selected device. Automations include:

- Force all applications to close and reboot the focus system.
- Run automations on the focus system via Silent, Prompt or Notify mode.
- Run Collection automations on the focus system.
- Run Engagements on the focus system.
- View the Automation History.
- View the Collection Extension History.

Administrator Actions

This tab displays the available actions that can be run on endpoint systems. The reboot action is automatically available on this tab. Users with appropriate rights can use the Reboot action to reboot the focus system (the endpoint system that you are currently viewing in Device Lookup). You need to customize any additional administrative actions thatyou want to use on this tab.

If desired, you can also customize this tab to add your own administrative actions. SeeCreating Custom Actions for more information.

Sensor Actions Tab

A Sensor Action is a template that can be executed on the focus system. Sensor Actions can be configured to run automatically when a sensor is activated, and can also be run manuallyfrom the Sensor Actions tab.

Execute a Sensor Action

To execute a sensor action, select an action template in the grid, enter any parameter values in the Execution Parameters section, select the desired User Interaction, and click theExecute button.

The following behaviours correspond with each User Interaction.

- **Run Silently** causes the action to run without notifying the user.
- **Prompt** sends the user a notification that the action is about to run.The user can accept or decline the action.

You will not be notified if the user declines the action.

- **Notify** sends a notification that the action is about to run without giving the user the option to accept or decline the action.

Automation History

This list includes up to the last five views you have visited during the current Device Lookup session. You can hover over each list item to display which user and system was theselected focus for the view.

Each list item is a link you can click to return to the view (for the indicated user's system).

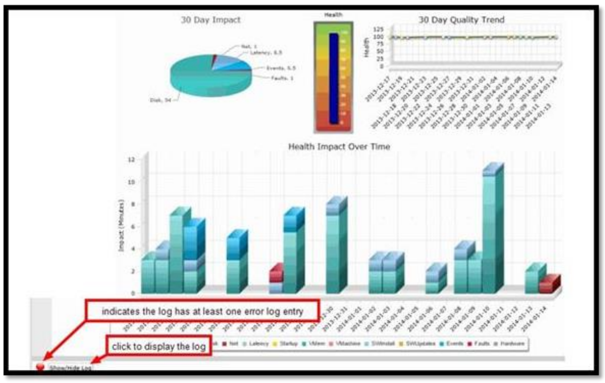
View the Log

Most Device Lookup log entries are informational only, and no action is required. But if an error is added to the log that you cannot Device Lookup yourself, you can export the log tofile and then share the file with Technical Support.

Entries are added to the log on a per session basis; they are refreshed if you close andthen reopen Device Lookup

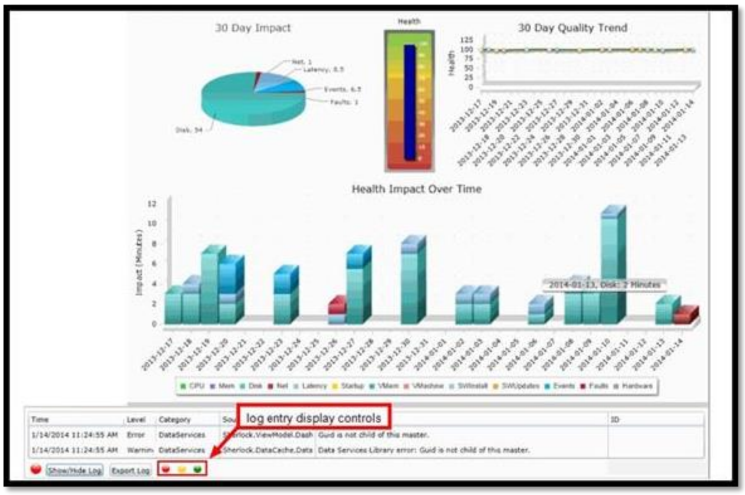
When you open Device Lookup the log is not displayed by default. Todisplay the log, click the Show/Hide Log button in the lower-left corner of anyDevice Lookup screen

A red circle (as shown below) indicates that the log has at least one error entry. Ayellow circle indicates the log has at least one warning entry, but no error entries. A green circle indicates the log has no error or warning entries.



4. The log displays. You can use the log entry display controls to determinewhich log entry categories displays.

    a. Click the red control circle to display only error log entries.
    b. Click the yellow control circle to display only warning log entries.
    c. Click the green control circle to display all log entries.



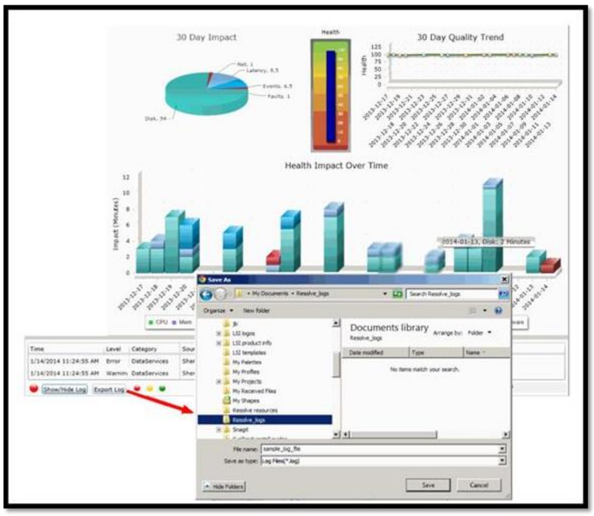
Time	Level	Category	Sou		ID
1/14/2014 11:24:55 AM	Error	DataServices	Sherlock.ViewModel.Dash	Guid is not child of this master.	
1/14/2014 11:24:55 AM	Warnin	DataServices	Sherlock.DataCache.Data	Data Services Library error: Guid is not child of this master.	

● Show/Hide Log   Export Log   ● ● ●

To export the log to file:

5. Click Export Log.
6. Use the resulting dialog box, navigate to the location where you wish to save the file.

7. Enter a user-defined File name for the log file.



```
Time                    Level   Category      Sour
1/14/2014 11:24:55 AM   Error   DataServices  Sher
1/14/2014 11:24:55 AM   Warnin  DataServices  Sher
```

File name: sample_log_file

Save as type: Log Files(*.log)

8. Click **Save.**

9. Click the **Show/Hide Log** button again to close the log.

Common Device Lookup Use Cases

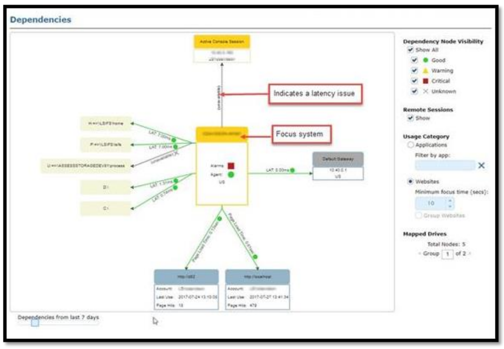
Slow System Response Time

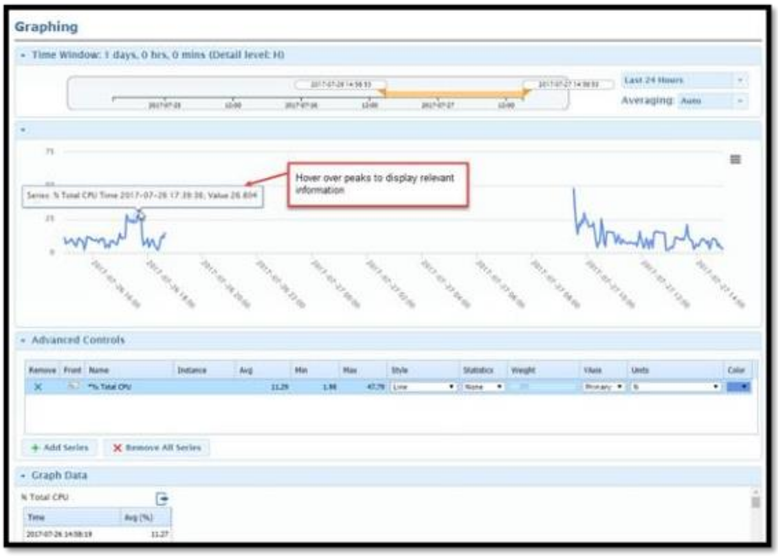
There are many different causes for a slow system response time. The steps below provideone path of many you could follow to investigate the issue.

1. Select the focus system associated with the trouble ticket.
2. Device Lookup connects directly to the selected system and executes a diagnosticroutine. The Overview screen opens, displaying the system's diagnostic results. Review any Diagnostic Categories with critical or warning level rules that provide clues such as the critical level Disk Use rule shown below. When you hover over arule, a description and recommended corrective action is provided.

The Health Tool helps you determine which categories are impacting the system's health that could be contributing to a slow system response time. The Total Impactgraph breaks out the categories that have impacted the system's performance. Thevalue displayed for each category is the total number of minutes the category has impacted the system's performance over the last 30 days. In the example shown below, notice that Latency is a relatively large contributor. Hovering over the Daily Impact bar graph provides the total number of minutes the category has impacted the system's performance over the last 30 days. The bars at each date point are broken into color coded category segments, hovering over a category segment displays the category's impact minutes for the indicated date.

The tool you use next to continue your investigation depends on the Health categories that have the highest impact on the system's health that could be contributing to a slow system response time. If Latency is having a high impact as shown above, you could then continue your investigation using the Dependencies Tool. This tool provides a system dependency map that includes a history of systems used to access the targeted system, local and mapped drives, and application dependencies and network latencies.

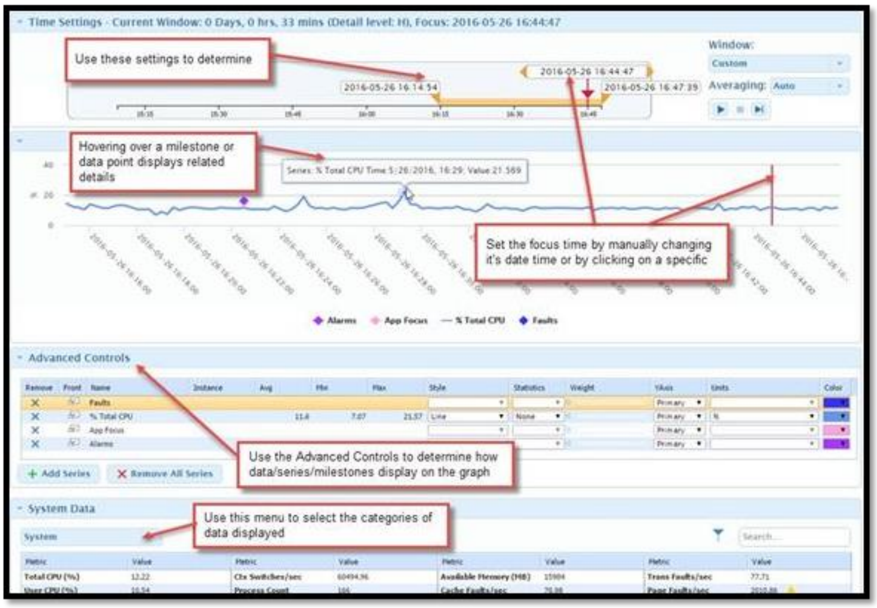



Graphing
Time Window: 1 days, 0 hrs, 0 mins (Detail level: H)
Last 24 Hours
Averaging: Auto
Hover over peaks to display relevant information
Series: % Total CPU Time 2017-07-26 17:39:38; Value 26.804
Advanced Controls
Add Series
Remove All Series
Graph Data
% Total CPU

Remove	Front	Name	Instance	Avg	Min	Max	Style	Statistics	Weight	YAxis	Units	Color
✕		% Total CPU		11.29	1.98	47.79	Line	None		Primary	%	

Time	Avg (%)
2017-07-26 14:38:19	11.27

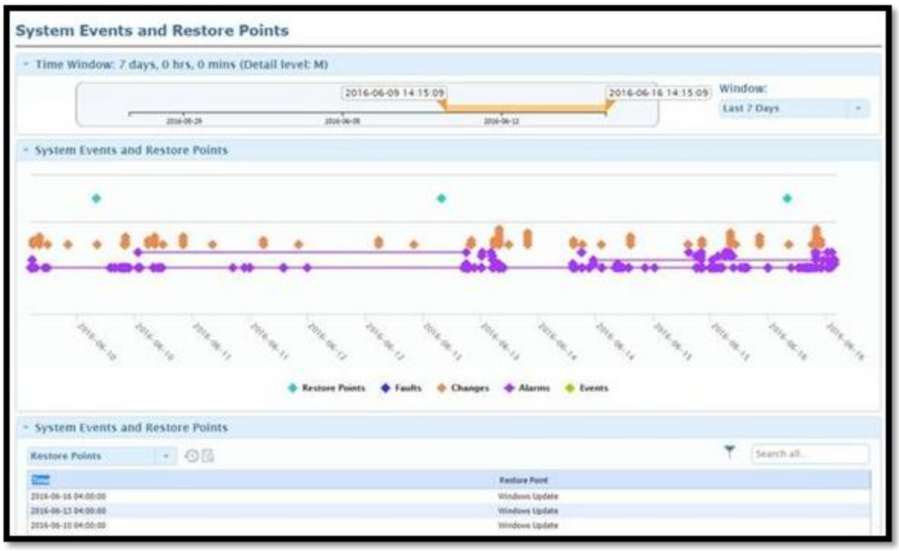
To instead investigate why the Health Tool Disk category has a high impact, you could use the Graphing Tool. This tool generates graphs for selected system data series and milestones over a specified time range. Multiple graphs are overlaid, allowing you to easily view and compare related concerns. It would be helpful to add relevant data series to the graph such as % Disk Time, Disk Queue Length, or Disk Transfer Time (%Total CPU displays on the graph by default). These are metrics that could cause slow performance, especially for a virtual machine. Notice the % Total CPU and Disk Queue Length extreme peaks on the graph – these would warrant further investigation. Hovering over data points displays relevant information. You could note the time the peaks occurred and use the Black Box Tool or the Event Correlation Tool to continue the investigation.


Time Settings - Current Window: 0 Days, 0 hrs, 33 mins (Detail level: H), Focus: 2016-05-26 16:44:47
Use these settings to determine
2016-05-26 16:14:54
2016-05-26 16:44:47
2016-05-26 16:47:39
Window:
Custom
Averaging: Auto
Hovering over a milestone or data point displays related details
Series: % Total CPU Time 5/26/2016, 16:29; Value 21.569
Set the focus time by manually changing it's date time or by clicking on a specific
Alarms
App Focus
% Total CPU
Faults
Advanced Controls
Use the Advanced Controls to determine how data/series/milestones display on the graph
Add Series
Remove All Series
System Data
System
Use this menu to select the categories of data displayed
Search...

Remove	Front	Name	Instance	Avg	Min	Max	Style	Statistics	Weight	YAxis	Units	Color
✕		Faults								Primary		
✕		% Total CPU		11.4	7.07	21.57	Line	None		Primary	%	
✕		App Focus								Primary		
✕		Alarms								Primary		

Metric	Value	Metric	Value	Metric	Value	Metric	Value
Total CPU (%)	12.22	Ctx Switches/sec	60494.96	Available Memory (MB)	15904	Trans Faults/sec	77.71
User CPU (%)	10.54	Process Count	166	Cache Faults/sec	75.98	Page Faults/sec	2010.88

Further analysis can be performed using the Black Box Tool. This tool allows you to review detailed system data for a specific point in time (the Focus Time). You could, for example, set the Focus Time to the point where multiple alarms display. Hovering over an alarm displays relevant details.



System Events and Restore Points

Time Window: 7 days, 0 hrs, 0 mins (Detail level: M)

2016-06-09 14:15:09 — 2016-06-16 14:15:09

Window: Last 7 Days

System Events and Restore Points

System Events and Restore Points

Restore Points

Search all...

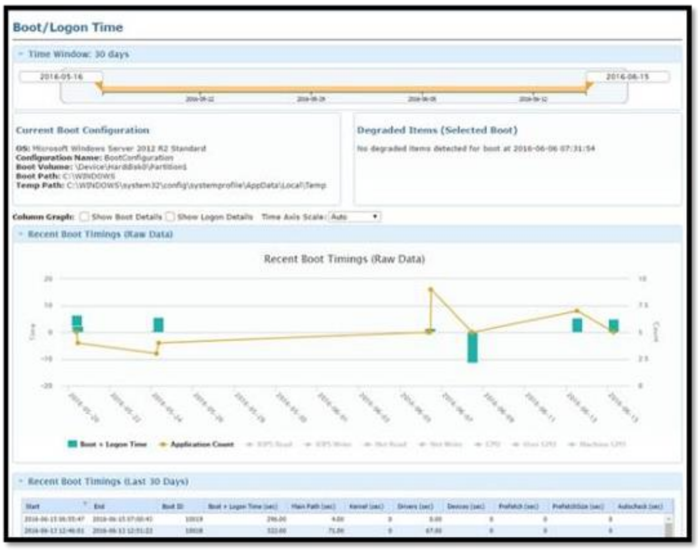
Time	Restore Point
2016-06-16 04:00:00	Windows Update
2016-06-13 04:00:00	Windows Update
2016-06-10 04:00:00	Windows Update

The Event Correlation Tool is also a useful investigative tool. This tool over lays fault eventsand system alarms with system changes that occurred during the same specified time frame. Additionally, this tool has an option that allows you to roll the system back to a restore point before the issues occurred.

Start Up Application and Boot Time Issues

The Boot/Logon Time Tool and Logon Process Tool can be used to track reported start upapplication and boot time issues.

1. Select the focus system associated with the trouble ticket.
2. Start with the Boot/Logon Time Tool to help identify the issue. This tool providesboot and logon data for the last thirty days. Using the data, you can determine ifthere are any specific issues that are causing slower boot times. Additionally, the tool's graph maps boot times to system login processes to assist in problem determination. Each of the graph stacked column components represents a different item in the boot sequence.



Boot/Logon Time

Time Window: 30 days

2016-05-16 — 2016-06-15

Current Boot Configuration

OS: Microsoft Windows Server 2012 R2 Standard
Configuration Name: BootConfiguration
Boot Volume: \Device\Harddisk0\Partition1
Boot Path: C:\WINDOWS
Temp Path: C:\WINDOWS\system32\config\systemprofile\AppData\Local\Temp

Degraded Items (Selected Boot)

No degraded items detected for boot at 2016-06-06 07:31:54

Column Graph: □ Show Boot Details □ Show Logon Details Time Axis Scale: Auto

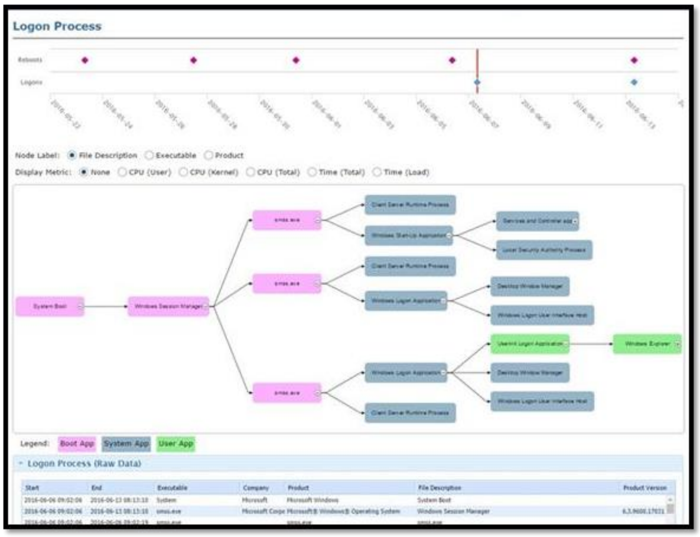
Recent Boot Timings (Raw Data)

Recent Boot Timings (Last 30 Days)

Start	End	Boot ID	Boot + Logon Time (sec)	Main Path (sec)	Kernel (sec)	Drivers (sec)	Devices (sec)	Prefetch (sec)	PrefetchSize (sec)	Autocheck (sec)
[illegible]	[illegible]	10019	296.00	4.00	0	3.00	0	0	0	
[illegible]	[illegible]	10018	322.00	71.00	0	67.00	0	0	0	

Hover over each Start-up stacked columns on the graph. If there were any issues that caused slower boot times for any of the graphed Start-ups, the issue details will display inthe Degraded Items pane. This detail information may be useful in tracking the start-up application and boot time issue.

After identifying a Boot/Logon issue and the time that it occurred, you can use the LogonProcess Tool to further investigate.



Logon Process

Node Label: ● File Description ○ Executable ○ Product

Display Metric: ● None ○ CPU (User) ○ CPU (Kernel) ○ CPU (Total) ○ Time (Total) ○ Time (Load)

Legend: Boot App System App User App

Logon Process (Raw Data)

Start	End	Executable	Company	Product	File Description	Product Version
2016-06-06 09:02:06	2016-06-13 08:13:10	System	Microsoft	Microsoft Windows	System Boot	
2016-06-06 09:02:06	2016-06-13 08:13:10	smss.exe	Microsoft Corpo	Microsoft® Windows® Operating System	Windows Session Manager	6.3.9600.17031

Reboots
Logons
2016-05-22
2016-05-24
2016-05-26
2016-05-28
2016-05-30
2016-06-01
2016-06-03
2016-06-05
2016-06-07
2016-06-09
2016-06-11
2016-06-13
System Boot
Windows Session Manager
smss.exe
smss.exe
smss.exe
Client Server Runtime Process
Windows Start-Up Application
Services and Controller app
Local Security Authority Process
Client Server Runtime Process
Windows Logon Application
Desktop Window Manager
Windows Logon User Interface Host
Userinit Logon Application
Windows Explorer
Windows Logon Application
Desktop Window Manager
Windows Logon User Interface Host
Client Server Runtime Process

The pink diamond icons on the **Milestones** chart represent system reboots, and the blue icons represent **Logons**. Hovering over an icon displays the time stamp for the event. Click to select the logon milestone that has the date corresponding to the date of the discoveredBoot or Logon issue. This displays the executables that start up when the selected session started in the Logon Process Tree and displays the data in tabular format for the start up inthe Logon Process (Raw Data) table

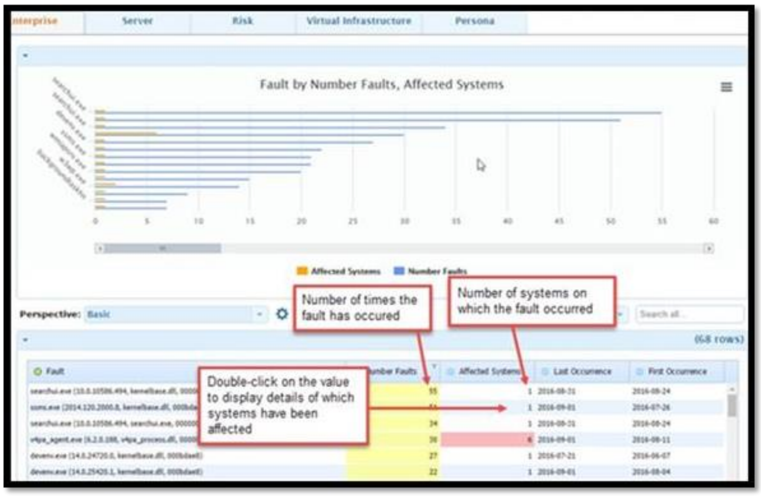
Click any of the Logon Process Tree items to view details such as start and end time.

Scope of Application Faults

When more than one user reports application faults for the same application, it is a good practice to determine the scope of the issue (the number of users and the specific users affected by the application fault).

3. Use the Faults Tool to begin your investigation. This tool identifies software package faults that have impacted the system during the selected time range. If the scope of the fault is Systemic, the fault has occurred on at least one other system in the enterprise. If the scope of the fault is Isolated, the fault has only occurred on thefocus system. Systemic faults warrant further investigation. Begin by reviewing the information available about the fault and noting the date the systemic fault occurred.

4. Using the Application Faults dataset, find the fault that occurred on the date you noted. You can quickly determine which systems have been affected by the fault by right-clicking on the Affected Systems value, and then selecting Show Details.



Number of times the fault has occured

Number of systems on which the fault occurred

Double-click on the value to display details of which systems have been affected

Fault	Number Faults	Affected Systems	Last Occurrence	First Occurrence
searchui.exe (10.0.10586.494, kernelbase.dll, 0000	55	1	2016-08-31	2016-08-24
ssms.exe (2014.120.2000.8, kernelbase.dll, 000bda	[illegible]	1	2016-09-01	2016-07-26
searchui.exe (10.0.10586.494, searchui.exe, 00000	34	1	2016-08-31	2016-08-24
v4pa_agent.exe (6.2.0.188, v4pa_process.dll, 0000	30	6	2016-09-01	2016-08-11
devenv.exe (14.0.24720.0, kernelbase.dll, 000bdaed)	27	1	2016-07-21	2016-06-07
devenv.exe (14.0.25420.1, kernelbase.dll, 000bdaed)	22	1	2016-09-01	2016-08-04

4.5 Device Manager

Overview

Devices represent the PC devices that are in your organization and typically used byemployees. A device can be a tablet, notebook, desktop, workstation, or more.

4.5.1 Add Devices

Adding a device requires providing details to the portal about the device (serial number,model, etc.) and provisioning the device with configuration and a software agent.

4.5.2 Manage Devices

Devices in your organization's portal can be accessed via **Device Manager → Devices**.

Each device in the table represents a device that was added into your portal, including devices that have not yet completed registration. The Status for each device is helpful foridentifying the expected functionality for the device. For the device status, refer to Track Device on LDI.

View Devices

Device Tray

From the Devices page, click on any device to open its corresponding *Device Tray*. The Device Tray contains following tabs:

- Device details
- Activity History

The following options are available for a user on the Device Tray:

- View device details
- View hardware and software details about this device
- Delete the device
- Raise a support ticket
- Crashes & Unsafe Shutdowns
- Installed Components & Versions

The following options are available on the device tray - *Activity History* tab:

- View the device Activity History
- Export device Activity History to CSV file
- Delete device

Installed Components and Versions (BIOS, Drivers, Firmware)

- Current BIOS Version
- List of device drivers loaded in last 7 days including current version
- Firmware
- Operating System

4.5.2.1. Delete or Remove a Device

A device should be unclaimed if you want to remove it from your portal, especially when ownership of the device will be transferred outside of your company.

1. Select the devices in the devices list.
2. Click **Delete** and confirm.

The device is no longer accessible in your portal. We recommend you uninstall the LDI Agent from the device if you do not want to use the device in the portal.

4.5.2.2. Rename a Device

1. Select Device Manager → Devices.
2. Search the device by name or by label.
3. Select More → Export Device List. The Export Devices window appears.
4. Click **Yes**.
5. Open the downloaded CSV file and make the desired changes.
6. Select **More → Import Device Changes**. The **Import Device Changes** windowappears.
7. Select the file to import and click **Verify**. The **Import Devices** window appears.
8. Click **Yes**. The **Import Device Changes** notification window appears stating that the details are sent to your email ID.

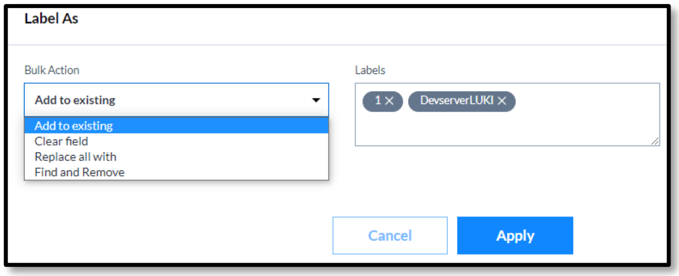
9. Click **Close**.

Note: Once you receive an email, confirm the change.

Device Labels

To group the devices based on department, location, or device type, you label them using the Label As feature.

1. Select Device Manager → Devices.
2. Select one or more devices and click **Label As**.



Label As

Bulk Action: Add to existing

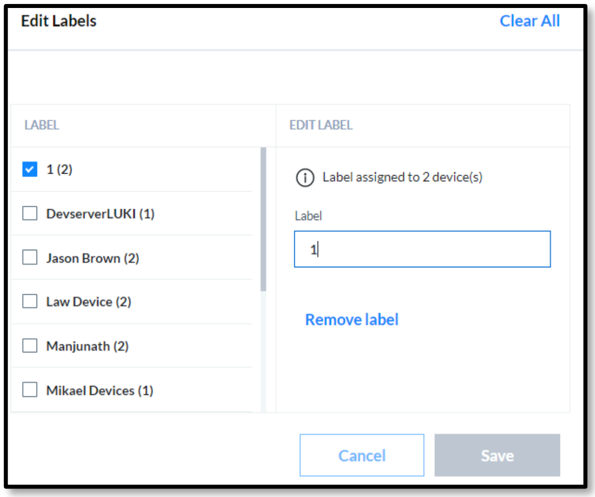
Labels: 1 ×, DevserverLUKI ×

3. Select a value from the **Bulk Action** drop-down list and click in the **Labels** field to select an existing label or create a new one.
4. Click **Apply**. The label/labels are assigned to the device/devices.

Edit Labels

You can edit or delete a label using the Edit Labels feature.

1. Select Device Manager → Devices.
2. Select More → Edit Labels.



Edit Labels

Label assigned to 2 device(s)

Label: 1

3. To remove a label, select one or more labels and click **Remove label**.

Note: From any of the pages that have the filtering widget, you can filter the devices based on label.

4.5.3 Notifications

4.5.3.1. Email Notification on Fleet

The portal sends daily email reports summarizing the issues that are reported in the Dashboard to all users enrolled in your organization. By default, the **Daily Email Summary** report is enabled. Preferences for E-mail Notifications can be configured byselecting User Icon → **Preferences** in the top ribbon.

Feedback

We value all feedback from users**.** A feedback form can be accessed by clicking on the Messaging Icon (💬) in the top ribbon.

4.5.3.2. Customize Alarms and events

When you select an alarm category button from the Alarm Dashboard, the table displays data for the category's alarms that were active at the Focus Time. Active alarms are thosewith critical (red) or warning (yellow) severity levels.

When you select the Alarms category, data for the last alarm category button selected displays.

5 Remediation Automation

5.1 Purpose

This chapter helps you understand how to configure, automate, and schedule automatically triggered remedial actions for issues detected in the specific device(s) or fleet of devices.

This chapter focuses mainly on how to trigger remedial actions:

- Automatically by a schedule when a selected sensor is activated.
- Manually on a specific device.
- Manually on all the devices in the fleet that have the same sensor activated.

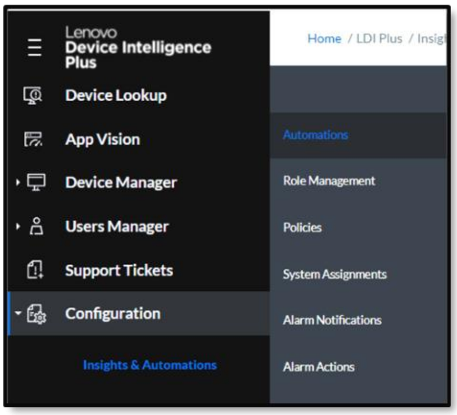
5.2 Audience

The guide is intended for IT Administrators, Managers, and Analysts.

5.3 Overview

The Workflow Automation module in the LDI Plus navigation menu allows you to configure LDI Plus for your business processes. You can import a remedial action in the LDI account, which automates an imported action and schedule it to run on a device or fleet of devices to automatically resolve a specific issue. For example, you can automate the restart of selected devices, whenever a specific issue occurs.

The Actions can also be manually executed on a device or fleet of devices.



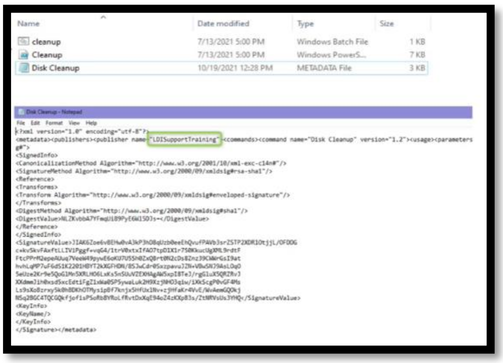
Upload a remediation script and assign automation to it to trigger an automatic response for a specific issue, whenever it occurs in the device or fleet of devices. A remediation script is Lscmd file that contains:

- PowerShell script
- .bat file to execute.ps1 script

- .metadata file

To create and enable a script, you need a pair of public-private keys. You must raise a key to CSW ticket for Lscmd file to be bundled and/or pair of public-private keys.

Note: The metadata file must contain the correct Publisher name value that matches with the public key publisher's name. This mandatory requirement for the approval of the remediation script (Action). For example, LDISupportTraining is the Publisher name value mentioned the Disk Clean up script.



Name	Date modified	Type	Size
cleanup	7/13/2021 5:00 PM	Windows Batch File	1 KB
Cleanup	7/13/2021 5:00 PM	Windows PowerS...	7 KB
Disk Cleanup	10/19/2021 12:28 PM	METADATA File	3 KB

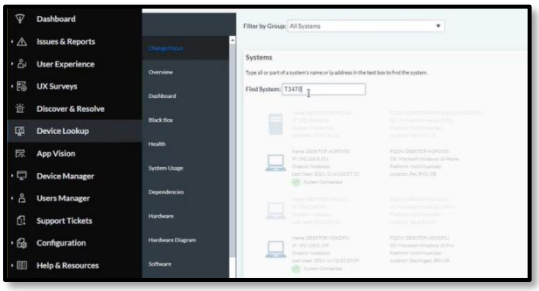
```
<?xml version="1.0" encoding="utf-8"?>
<metadata><publishers><publisher name="LDISupportTraining"<commands><command name="Disk Cleanup" version="1.2"><usage><parameters
g#">
<SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<Reference>
<Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>NLZKvbbA7YFmqUi89PyE6W15DJs=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>JIAK6Zoe6vBEHw0vA3kP3hO8qUzb0eeEhQvufPAVb3srZSTP2XDR1OtjjL/OFDOG
c+kvSkvFAxftLLIV1Pggf+vqG4/1trV0xtxIfAO7tpD1X1r7S0KkucUgXML9rdtF
FtcPPrM2epeAUuq7VeeW49pywE6oKU7USSh0ZxQ8rt0N2cDs8Znz39CWWrGsI9at
hvhLqMP7uF6dS1K2201HBYT2kXGFHDN/8SJwCdr0SxzpavuJZN+VBwSN79AsLOqO
5eUze2Kr9e5QoG1Mn5XRLHO6LxKs5nSUuVZEXHAgAW5xpI8Te3/rgGluX5QRZRvJ
XXdmmJih0xsd5xcEdtiFgZ1xWa0SP5ywaLuk2H9XzjNHO3qiw/iXk5cgP0vGF4Ms
Ls9sXo8zrxy5k0hBDKhOTMysip8f7knjx5HfUx1Nv+zjHfaKr4VvE/WvAemGQOkj
NSq2BGC4TQCGQkfjofisPSoRb8YRoLfRvtDxXqE94oZ4zKXp83s/ZtNRVsUs3YHQ</SignatureValue>
<KeyInfo>
<KeyName/>
</KeyInfo>
</Signature></metadata>
```

Example of Remediation script for Disk Clean-up

5.4 Manually Resolve Issues

5.4.1 Run a Remedial Action Manually on a Specific Device

1. In the **Device Lookup** page, search for a desired device.



Filter by Group: All Systems

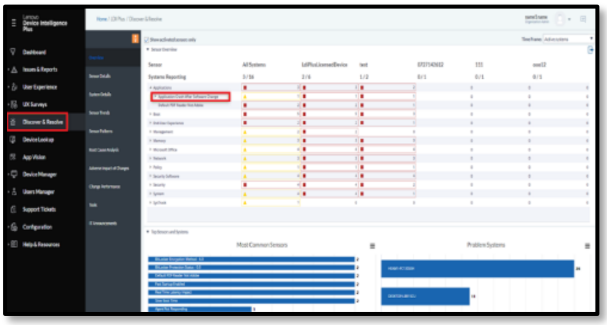
Type all or part of a system's name or ip address in the text box to find the system.

Find System: T3470

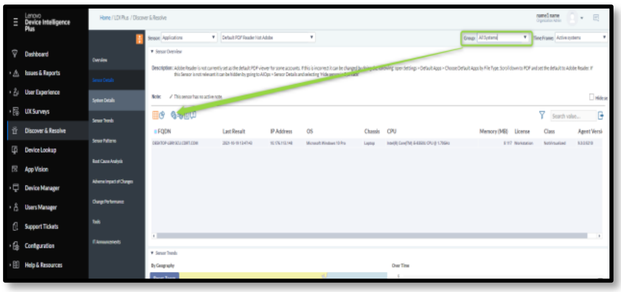
2. Click **Tools**, select **Run Automations** tab, and then run the created automation from the list.

5.4.2 Run a Remedial Action Manually on All the devices in the Fleet When a Selected Sensor is Activated

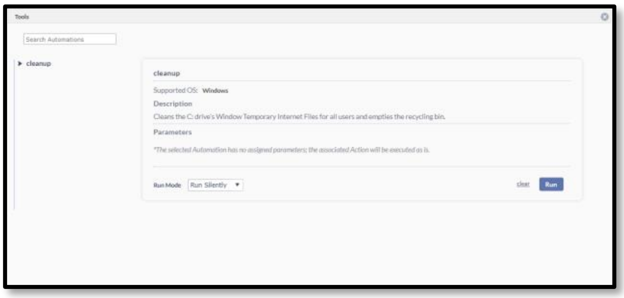
1. In the **Discover & Resolve** page, double-click any sensor reproducible on at least one device.



2. Select the device group like All Systems, and then click the **Gear** icon.



3. Select the created automation and click **Run**.



cleanup

Supported OS: Windows

Description

Cleans the C: drive's Window Temporary Internet Files for all users and empties the recycling bin.

Parameters

*The selected Automation has no assigned parameters; the associated Action will be executed as is.

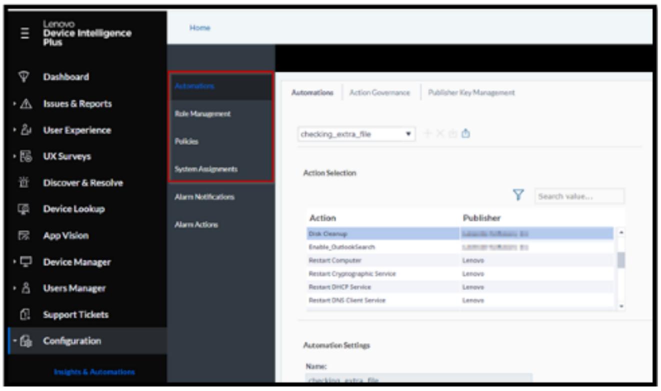
Run Mode: Run Silently ▾

Note: Select **Device Lookup → Tools** to view the list of executed automations with return code (execution result) and additional information.

5.5 Configure System to Self-Heal

The Remediation Automation chapter provides you the details of how to import a remedial action, configure it, and assign automation to it. The following sub modules help you to take the desired actions:

- Automations - Approve an imported action and assign automation to it.
- Role Management - Set up a schedule for the execution of automated action(s).
- Policies - Assign roles to the configuration. The configuration is a set of roles assigned to selected devices or a fleet of devices.
- System Assignments - Assign configuration to device(s) or system of devices.



checking_extra_file

Action Selection

Action	Publisher
Disk Cleanup	[redacted]
Enable_OutlookSearch	[redacted]
Restart Computer	Lenovo
Restart Cryptographic Service	Lenovo
Restart DHCP Service	Lenovo
Restart DNS Client Service	Lenovo

Automation Settings

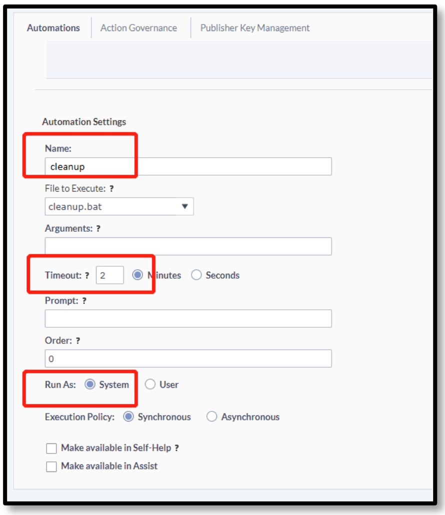
Name: checking_extra_file

5.5.1 Clean up Temporary and Recycle Bin Files

Note: To run the remediation action, you must configure the corresponding automation, otherwise the **Clean** button is disabled.

1. Select **Configuration → Insights & Automations**.
2. Click **Automations**.
3. Perform the Automation Settings using the standard action **Disk_ Cleanup**.

Note: Refer Assign Automation to the Action for assigning automation to an action. If the **cleanup.bat** action is not available in the **Action Documentation**, you must upload it from the pack.



Automation Settings

Name: cleanup

File to Execute: ? cleanup.bat

Arguments: ?

Timeout: ? 2 ● Minutes ○ Seconds

Prompt: ?

Order: ? 0

Run As: ● System ○ User

Execution Policy: ● Synchronous ○ Asynchronous

□ Make available in Self-Help ?

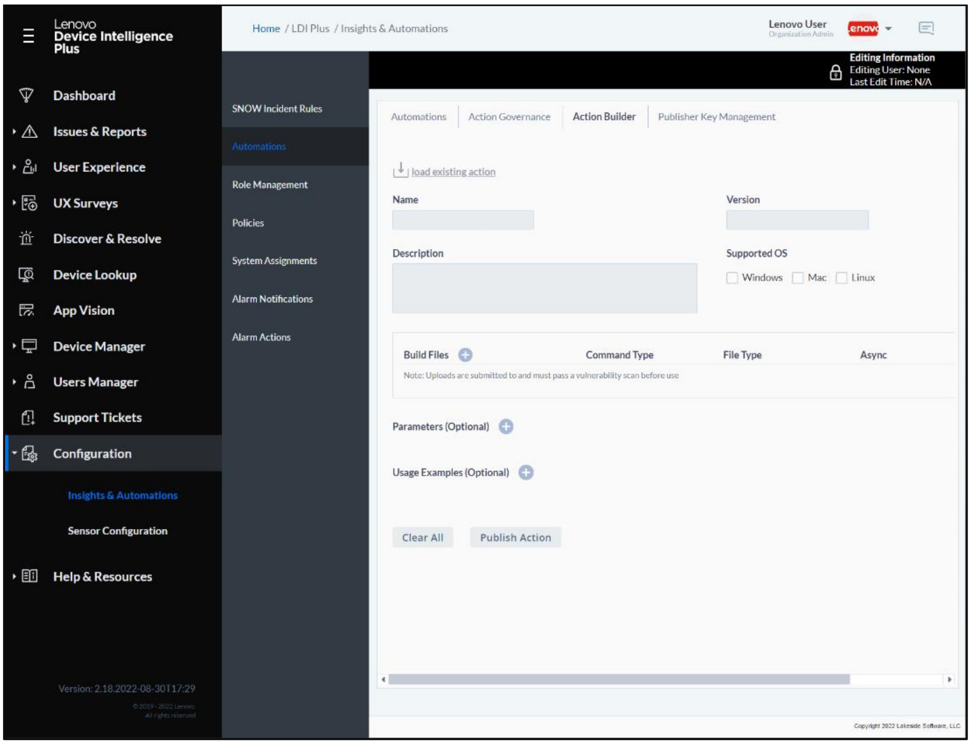
□ Make available in Assist

To import an Action and assign automation to it, follow these steps:

5.6 Action Builder

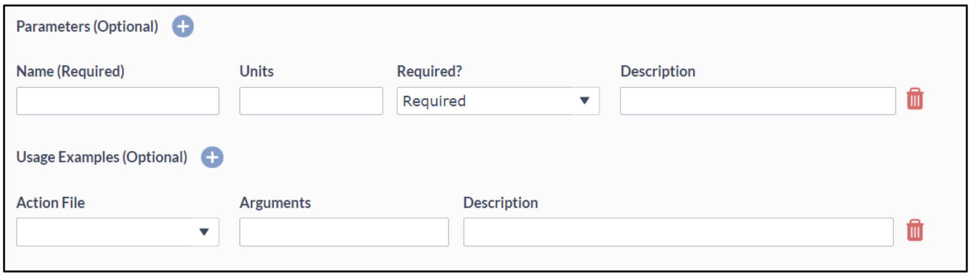
The Action Builder section provides you the ability to build, configure, and publish custom actions.

1. To build your custom actions, begin by navigating to Configuration → Insights & Automations → Automations and select the “Action Builder” tab at the top.
2. Next, unlock the page by clicking the padlock icon in the top right of your screen.

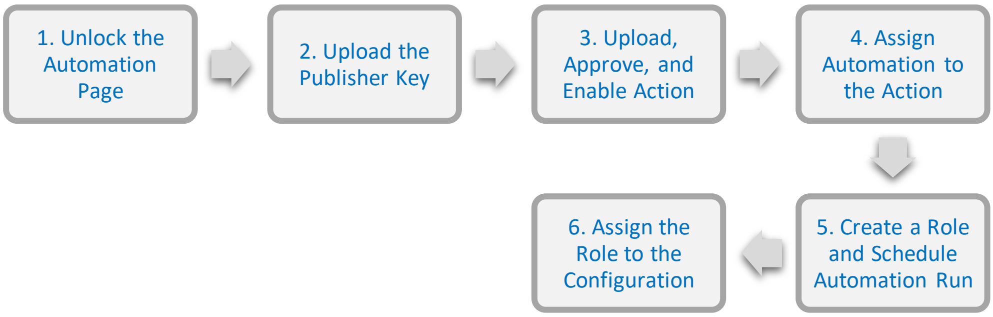


3. Give a **Name** to the action.
4. Define the **Version**, **Description**, and **supported OS**.
5. Attach the PowerShell script by clicking on **Build Files**.

   Note: The Parameters and Usage Examples are optional but are useful to understand the action.



5.7 Run a Remedial Action Automatically by a Schedule when a Selected Sensor is Activated



1. Unlock the Automation Page

2. Upload the Publisher Key

3. Upload, Approve, and Enable Action

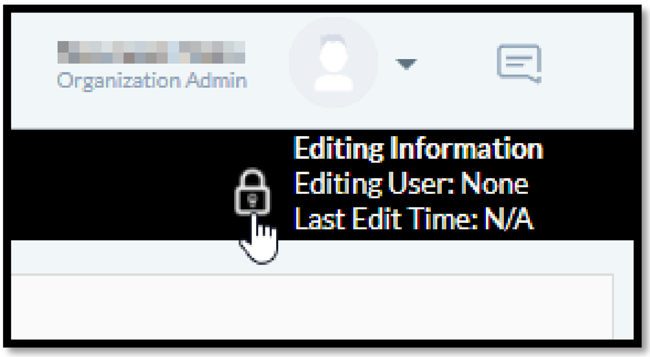
4. Assign Automation to the Action

5. Create a Role and Schedule Automation Run

6. Assign the Role to the Configuration

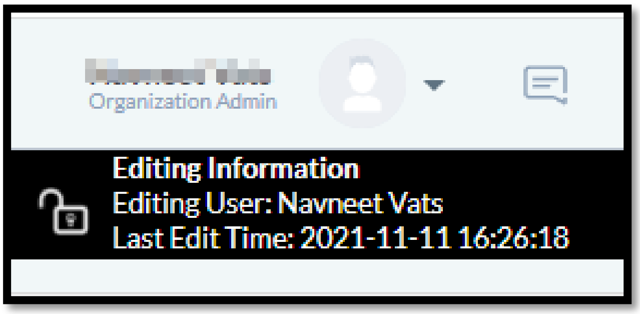
5.7.1 Unlock the Automation Page

1. Click the **Lock** icon to unlock the default Automation page.



Editing Information
Editing User: None
Last Edit Time: N/A

The lock in unlocked.



Editing Information
Editing User: Navneet Vats
Last Edit Time: 2021-11-11 16:26:18

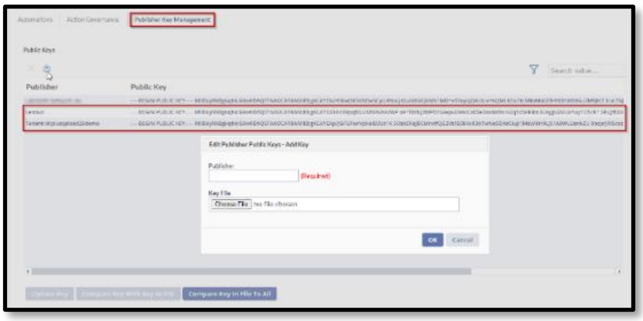
5.7.2 Upload the Publisher Key

The Actions in the Action table are preloaded by Lenovo for the LDI Plus user. The preloaded Actions are signed by the Public-private key pair. If you want to create a new Action that is not provided by Lenovo, then you need publisher key to approve that Action.

If the publisher changes the public key, you can update it. Click **Update Key**, select the key, and then click **OK**.

Note: In the **Automations** page, the publisher's name must match the publisher's name for an Action.

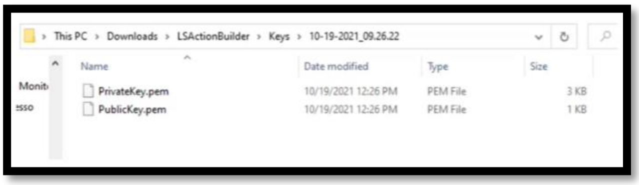
1. Click **Publisher Key Management**. The Public Keys pane appears.



2. Click **Upload**. The **Add Key** modal window appears.
3. Select the file.
4. Click **OK**.

Note

- You must upload the public key to approve an Action.
- You need private key to sign into the script.



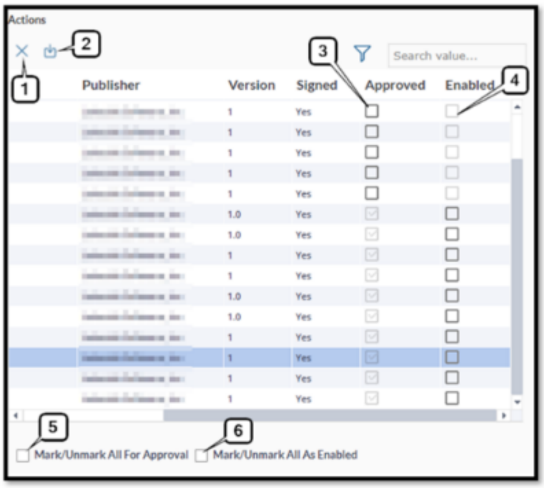
› This PC › Downloads › LSActionBuilder › Keys › 10-19-2021_09.26.22

Name	Date modified	Type	Size
PrivateKey.pem	10/19/2021 12:26 PM	PEM File	3 KB
PublicKey.pem	10/19/2021 12:26 PM	PEM File	1 KB

5.7.3 Upload, Approve, and Enable Action

Use the **Governance** tab to import new actions in the table and approve them. You cannot assign automation to action that is not approved. To approve, you must authenticate the action by signing in with a private and public key. For example, the remedial action has a public key, and the LDI admin user or publisher has a private key, which is matched against the public key to authenticate the action. The private key is necessary to create a signature against the metadata file. When the publisher approves the action, it verifies the signature of the metadata file against the public key to ensure that it was not modified. After validation, the Action metadata file is added to the Master data file, from where the endpoint systems again check the action metadata file before downloading it.

Note: The **Action Governance** tab allows you to import, delete, approve, enable, and disable actions.



Actions

Publisher	Version	Signed	Approved	Enabled
[illegible]	1	Yes	☐	☐
[illegible]	1	Yes	☐	☐
[illegible]	1	Yes	☐	☐
[illegible]	1	Yes	☐	☐
[illegible]	1	Yes	☐	☐
[illegible]	1.0	Yes	☑	☐
[illegible]	1.0	Yes	☑	☐
[illegible]	1	Yes	☑	☐
[illegible]	1	Yes	☑	☐
[illegible]	1.0	Yes	☑	☐
[illegible]	1.0	Yes	☑	☐
[illegible]	1	Yes	☑	☐
[illegible]	1	Yes	☑	☐
[illegible]	1	Yes	☑	☐
[illegible]	1	Yes	☑	☐

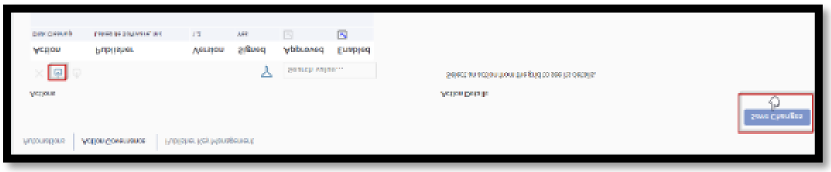
☐ Mark/Unmark All For Approval ☐ Mark/Unmark All As Enabled

1. **Delete icon** - Select the application and click the **Delete** ✕ icon. The Action is removed from the table. The Action is also removed from the endpoint configuration, whenever it is updated.
2. **Import icon** - Import an Action, which is a lscmd file made up of metadata file, a bat file, and a PowerShell script file, and signed by the pair of public-private keys.
3. **Approved checkbox** - Mark the checkbox to approve the Action. To approve an action, select the action, select the checkbox, and click **Save Changes**. On completion of the approval process, the Action is moved from the pending area to the area from where the endpoint systems can download the Action.

4. **Enabled checkbox** - Select the checkbox to enable the action. To enable the Action - **Select Action → select the checkbox → Click Save Changes**. On completion of the Enable process, the Action is downloaded on the endpoint systems.
5. **Mark or Unmark All for Approval checkbox** - Select the checkbox to approve all the Actions in the Action table. De-select the checkbox to undo the approval of Actions in the table.
6. **Mark or Unmark All As Enabled** - Select the checkbox to enable all the Actions in the table. De-select the check box to disable all the Actions.

Follow these steps to upload, enable, and approve an Action:

1. Click **Action Governance**. The Action Governance pane appears.



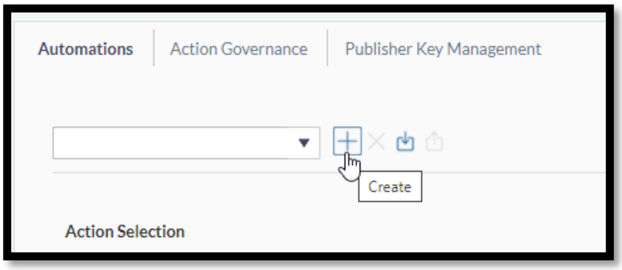
2. Click **Import**.
3. Select the remediation script file from your device.
4. Select the **Approved** checkbox.

Note: Upload the public key to approve the action.

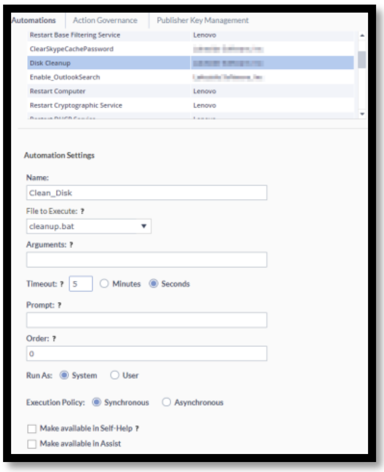
5. Select the **Enabled** Checkbox.
6. Click **Save Changes**.

5.7.4 Assign Automation to the Action

Use this tab to assign automation to an uploaded action.



1. Click **Automations**, and then click **Add**.
2. Select the Action from the Action table. For example, Disk Cleanup.



Restart Base Filtering Service	Lenovo
ClearSkypeCachePassword	[redacted]
Disk Cleanup	[redacted]
Enable_OutlookSearch	[redacted]
Restart Computer	Lenovo
Restart Cryptographic Service	Lenovo

Automation Settings

Name: Clean_Disk

File to Execute: ? cleanup.bat

Arguments: ?

Timeout: ? 5 ○ Minutes ● Seconds

Prompt: ?

Order: ? 0

Run As: ● System ○ User

Execution Policy: ● Synchronous ○ Asynchronous

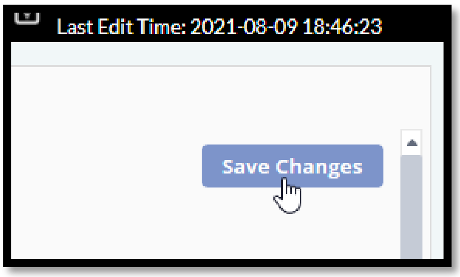
□ Make available in Self-Help ?

□ Make available in Assist

3. Enter the **name** of the Automation that you want to assign to the selected action. For example, Clean_Disk.
4. Select the type of executable file in the **File to Execute** field. For example, cleanup.bat. You can also enter constant and optional.
5. Select the Minutes or Seconds radio button and enter the time for which the action can run in the **Timeout** field. The maximum limit for timeout is 5 minutes. Select 0 if timeout is not needed.
6. Enter the text in the **Prompt** field. It is the text that appears on the screen of the end user before the action runs. Leave it empty if not required.
7. Enter the numeric value to point out the order in which the Action run in the **Order** field. Enter 1 to run the Action first or 2 to run it second.

Note: Select the **Synchronous** radio button if you want Actions to run in an order.

8. Select **System** radio button to run the Agent as the system in the **Run As** field. It has access to most system functions but is unable to interact with the UI. Select **User** radio button to allow logged user to interact with the UI.
9. Select **Synchronous** to run Actions in a specific order and if you have completed the previous step - **Order**. Select **Asynchronous** to run Multiple Actions, if applicable, for this same Automation, at the same time.



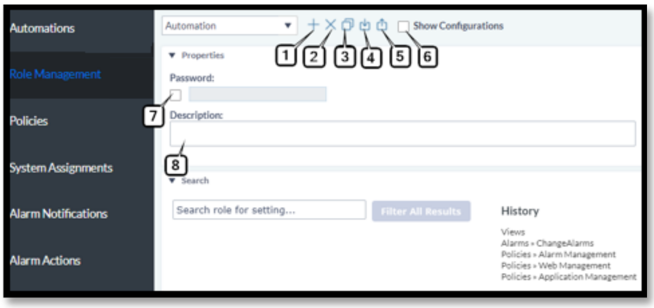
Last Edit Time: 2021-08-09 18:46:23

10. Click the **Save Changes** in the upper-right corner of the screen.

5.7.5 Roles

After you have created an automation, you need to define the role for the automation, and schedule the automation run.

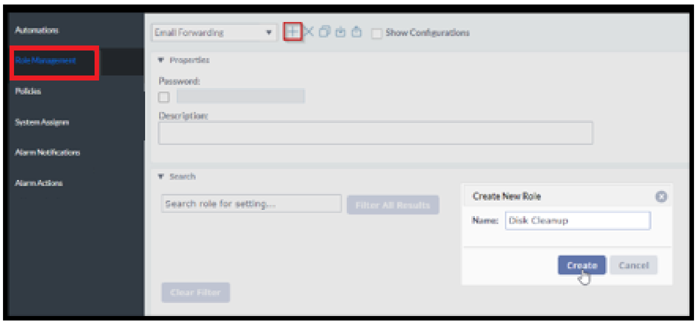
The role specifies various counters, alarms, events, etc., that are to be collected and alerted. One or more roles are grouped together to create configuration.



In the **Role Management** tab, you can do the following:

1. Create a new role.
2. Delete a role.
3. Copy a role.
4. Import a role.
5. Export a role.
6. Select this check box to view all the created roles in the drop-down list in the upper left corner.
7. Select this checkbox to view **Create New Password** pop-up window if you want to assign a password to the role.
8. Write a description of the role.

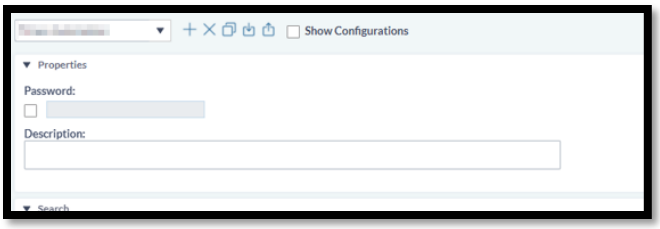
5.7.6 Create a Role and Schedule Automation Run



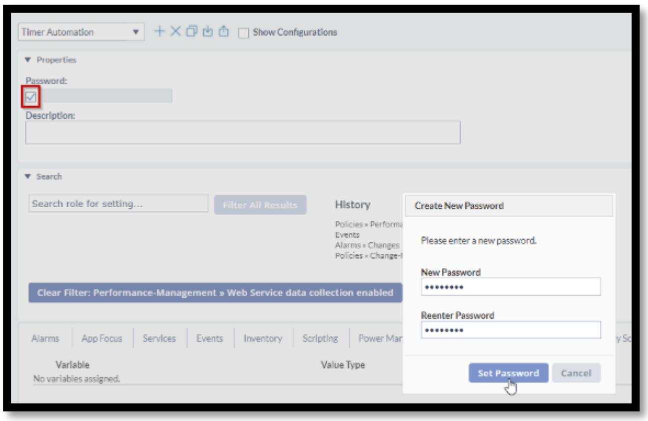
Name: Disk Cleanup

1. Click Role Management.
2. Click the **Add** + icon. A pop-up window appears.
3. Type the name of the role.
4. Click **Create**. A new role is created. For example, Disk Cleanup.

5.7.7 Assign Password to the Role (Optional)



You can also assign a password to the role to control who can view the role.



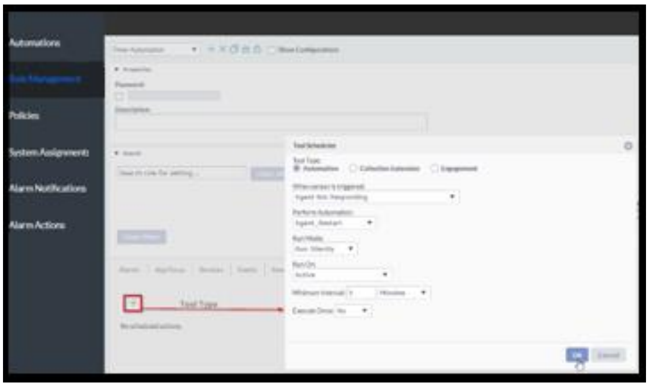
Please enter a new password.

New Password: ••••••••

Reenter Password: ••••••••

1. Select the **Password** checkbox. A pop-up window appears.
2. Enter the password.
3. Confirm the password.
4. Click **Set Password**. The password is created for the role.

5.7.8 Setup a schedule for automation run



You can set up one and more automations under a role.

1. Click Tool Schedules.
2. Click the **Add** + icon. The **Tool Schedules** pop-up window appears.
3. Select **Automation** in the **Tool Type** field.

4. In the **When sensor is triggered** drop-down list, select the type of sensor that gets activated and runs the automation. For example, Agent Not Responding.
5. In **the Perform Automation** drop-down list, select the Automation. For example, Agent_Restart is the automation that runs when the **Agent Not Responding** sensor is triggered.

Note: The **Perform Automation** list only displays Automations that have parameters that the sensor can provide.

6. Select how the automation is to be run from the **Run Mode** drop-down list.

> If you select Run Mode as:
>
> - **Run Silently** - No notification is sent.
> - **Prompt** - You get a prompt to click **OK** button before the automation can run.
> - **Notify** - Notifies you that the Automation runs after a countdown of one minute.

7. In the **Run On** drop-down list, you can select from three different options.

> If you select Run On as:
>
> - **Active** (default mode) – The automation makes a continuous run.
> - **When sensor activates** – The automation runs as soon as the sensor is activated.
> - **After Sensor is active** – The automation runs the moment, the duration of sensor activation is over.

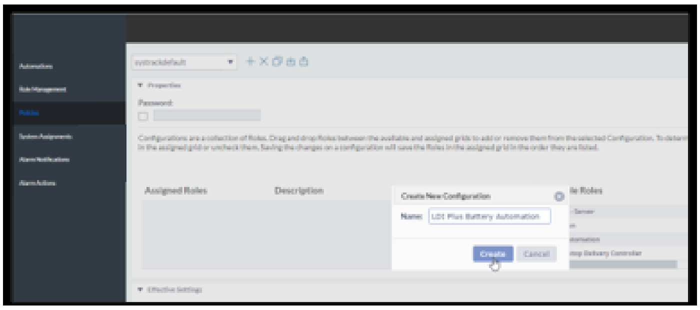
8. In the **Minimum Interval** field, enter the time in seconds, minutes, or hours. It is the frequency of repetition of the automation run.
9. Select Yes or No in the **Execute Once** drop-down list.

> If you select Execute Once as:
>
> - No – To have sensor run for every row in the sensor payload. For example, the sensor will run for all the applications that crash.

10. Click **OK**.
11. Click **Save Changes** in the upper-right corner of the page.

5.7.9 Assign Role to Configuration

Configuration is a collection of one or more Roles. You can create a new configuration and add existing roles to it.



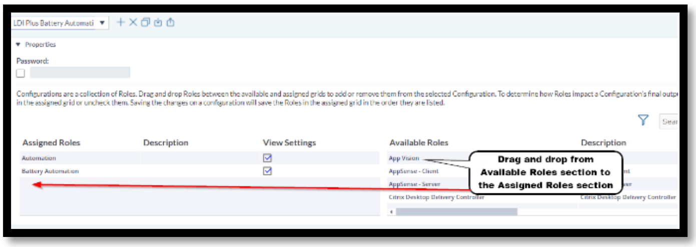
Name: LDI Plus Battery Automation

5.7.10 Create New Configuration

1. Click the Configurations tab.
2. Click the **Add** + icon. A pop-up window appears.
3. Enter the name of the configuration.
4. Click **Create**. A new configuration is created. For example, LDI Plus Battery Automation.

5.7.11 Add Roles in the Configuration

You can drag and drop the roles from **Available Roles** section to the **Assigned Roles** section to add the roles in the Configuration. You can adjust the order of the roles in the **Assigned roles** section by moving the rows, up or down.



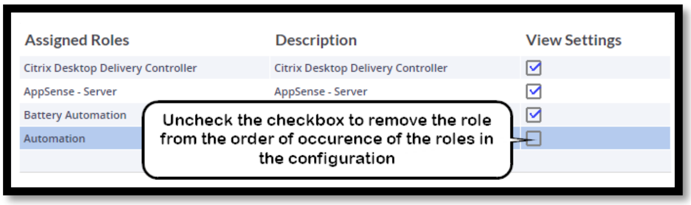
Configurations are a collection of Roles. Drag and drop Roles between the available and assigned grids to add or remove them from the selected Configuration. To determine how Roles impact a Configuration's final outp in the assigned grid or uncheck them. Saving the changes on a configuration will save the Roles in the assigned grid in the order they are listed.

Assigned Roles	Description	View Settings
Automation		☑
Battery Automation		☑

Available Roles	Description
App Vision	
AppSense - Client	
AppSense - Server	
Citrix Desktop Delivery Controller	Citrix Desktop Delivery Controller

Drag and drop from Available Roles section to the Assigned Roles section

To move a role in the section, select the row and then drag it to the desired position. You can adjust the order of occurrence of roles, by de-selecting the **View Setting** checkbox.



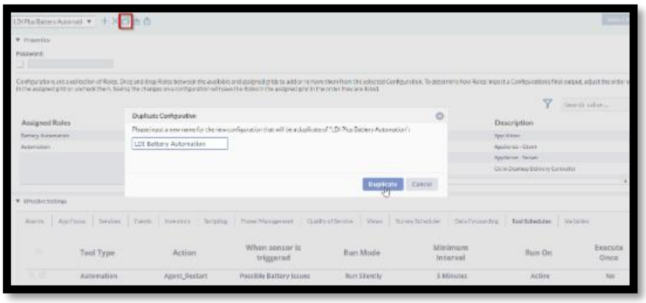
Assigned Roles	Description	View Settings
Citrix Desktop Delivery Controller	Citrix Desktop Delivery Controller	☑
AppSense - Server	AppSense - Server	☑
Battery Automation		☑
Automation		☐

Uncheck the checkbox to remove the role from the order of occurence of the roles in the configuration

5.7.12 Create a Duplicate Role

You can also create the duplicate of a role.

1. Click the **Duplicate** ⧉ icon.
2. Enter the name of duplicate role.
3. Click **Duplicate**. The duplicate role is created. For example, LDI Battery Automation is the duplicate of the *LDI Plus Battery Automation.*



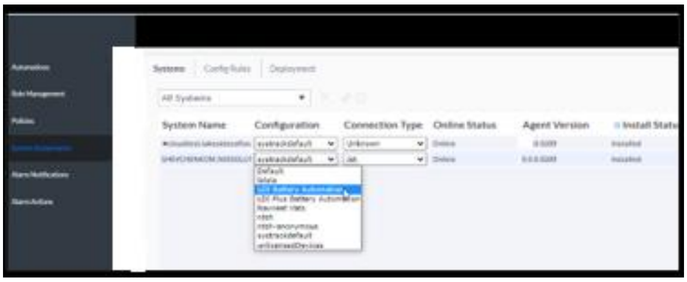
Please input a new name for the new configuration that will be a duplicate of "LDI Plus Battery Automation"

LDI Battery Automation

Tool Type	Action	When sensor is triggered	Run Mode	Minimum Interval	Run On	Execute Once
Automation	Agent_Restart	Possible Battery Issues	Run Silently	5 Minutes	Active	No

5.8 Assignments

When the creation of the configuration containing roles is completed, it can then be attached to a specific child machine or group of machines using Assignments.



1. Click **Assignments**. The **Systems** tab appears by default.
2. In the **Configuration** drop-down list, select a configuration. For example, LDI Battery Automation.
3. Click **Save Changes** in the upper-right corner. The new configuration is assigned to the child machine or system.

5.9 Alarm Automation

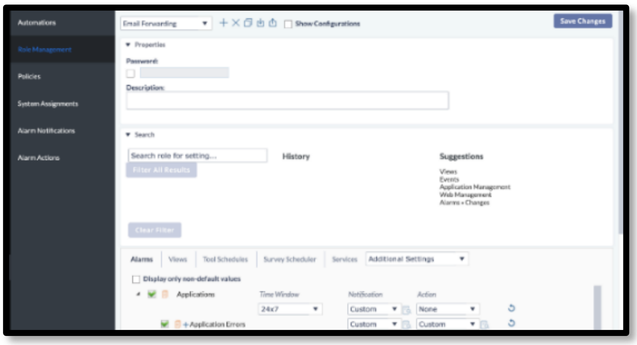
This feature allows you to receive email notifications when a certain issue occurs in a device. LDI Plus offers several events and alarms to configure detailed email notifications and automatic actions.

Pre-requisites

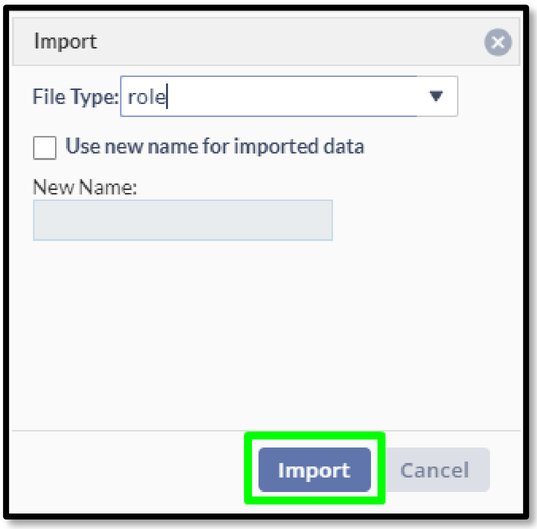
- Working SMTP server
- Email Forwarding role imported to the organization or available to be imported manually.

To automate an alarm

4. Select Configuration → Insights & Automations → Role Management.
5. In the top of the page, select **Email Forwarding** from the drop-down list.



6. In the **File Type** drop-down list, select role and click **Import**.

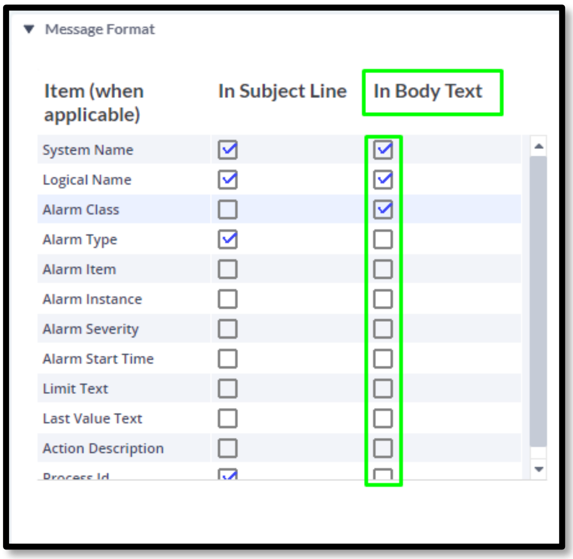


File Type: role

□ Use new name for imported data

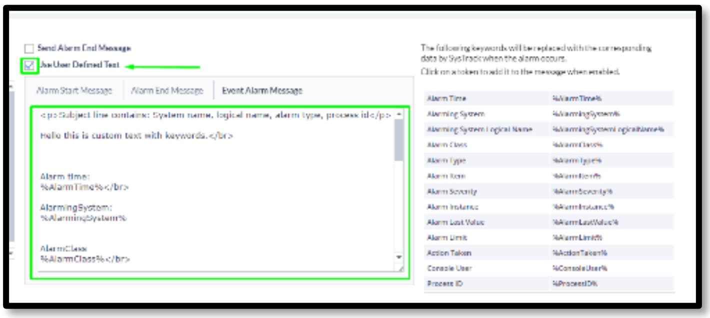
New Name:

7. In the **Alarm Notifications** page, do the following:
   - Create a notification setting profile.
   - Enable Email settings.
   - Fill out receivers of the alarm emails.
   - Configure the SMTP server and enable SMTP Authentication.
   - Enter sender’s email ID.
8. Configure the message format. If you do not configure it, the content of the email is defined by the selected checkboxes under **In Body Text**.



Item (when applicable)	In Subject Line	In Body Text
System Name	☑	☑
Logical Name	☑	☑
Alarm Class	□	☑
Alarm Type	☑	□
Alarm Item	□	□
Alarm Instance	□	□
Alarm Severity	□	□
Alarm Start Time	□	□
Limit Text	□	□
Last Value Text	□	□
Action Description	□	□
Process Id	☑	□

9. To configure the email manually, select **Use User Defined Text** and use the necessary template for the email. It is possible to select data from the list of keywords to be inserted into the email with valuable information.



□ Send Alarm End Message
☑ Use User Defined Text

```
<p>Subject line contains: System name, logical name, alarm type, process id</p>

Hello this is custom text with keywords.</br>


Alarm time:
%AlarmTime%</br>

AlarmingSystem:
%AlarmingSystem%


AlarmClass
%AlarmClass%</br>
```

The following keywords will be replaced with the corresponding data by SysTrack when the alarm occurs.
Click on a token to add it to the message when enabled.

Alarm Time	%AlarmTime%
Alarming System	%AlarmingSystem%
Alarming System Logical Name	%AlarmingSystemLogicalName%
Alarm Class	%AlarmClass%
Alarm Type	%AlarmType%
Alarm Item	%AlarmItem%
Alarm Severity	%AlarmSeverity%
Alarm Instance	%AlarmInstance%
Alarm Last Value	%AlarmLastValue%
Alarm Limit	%AlarmLimit%
Action Taken	%ActionTaken%
Console User	%ConsoleUser%
Process ID	%ProcessID%

10. When you configure an alarm message, you can choose from these available options: Alarm Start Message, Alarm End Message, and Event Alarm Message.

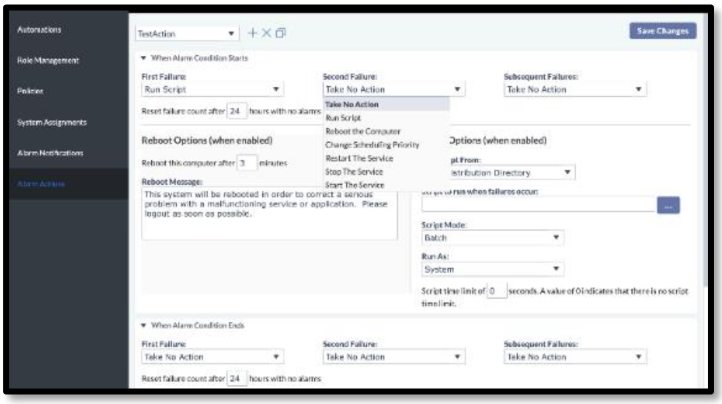
    An Alarm Start Message is triggered when a certain threshold is being met. For instance, if there is an alarm set for Disk Space, once a disk reaches a certain threshold, an Alarm Start Message is sent. Once that issue is solved, an Alarm End Message is sent, to notify an IT admin that an alarm is no longer active.

    An Event Alarm Message is triggered every time when a certain event occurs. For example, if there is an application crash, each time that application crashes, an Event Alarm Message is sent.

11. After configuring the alarm message, you should configure an Alarm Action, if needed. Alarm Action configuration is not required to receive an alarm notification via email. The purpose of an Alarm Action is to respond to a certain alarm. Here is a detailed description of how an Alarm Action can be configured:

    - Create and name an alarm action profile.

- Set alarm response for the first occurrence of an issue when an alarm condition starts.
- Set alarm response for the second occurrence of an issue. A list of all potential responses to a failure.
- Set alarm response for the subsequent occurrence of an issue.
  Set alarm responses when an alarm condition ends.
- Configure script options in case a Run Script option was chosen.



TestAction

When Alarm Condition Starts

First Failure: Run Script

Second Failure: Take No Action

Subsequent Failures: Take No Action

Reset failure count after 24 hours with no alarms

Reboot Options (when enabled)

Reboot this computer after 3 minutes

Reboot Message:

This system will be rebooted in order to correct a serious problem with a malfunctioning service or application. Please logout as soon as possible.

Options (when enabled)

pt From: istribution Directory

run when failures occur:

Script Mode: Batch

Run As: System

Script time limit of 0 seconds. A value of 0 indicates that there is no script time limit.

When Alarm Condition Ends

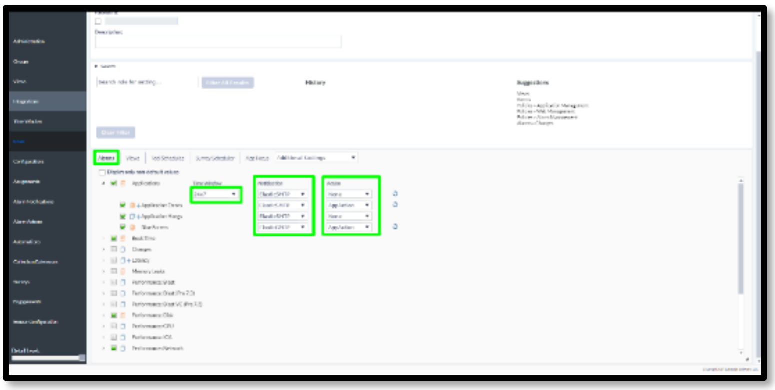
First Failure: Take No Action

Second Failure: Take No Action

Subsequent Failures: Take No Action

Reset failure count after 24 hours with no alarms

12. In the **Roles** page configure the alarms.



Each type of alarms can be configured individually. A set of alarms can be configured with a single notification profile or different ones. The Time window defines how long Lakeside analyses the device. Once everything is set up, save changes, and proceed to role configuration.

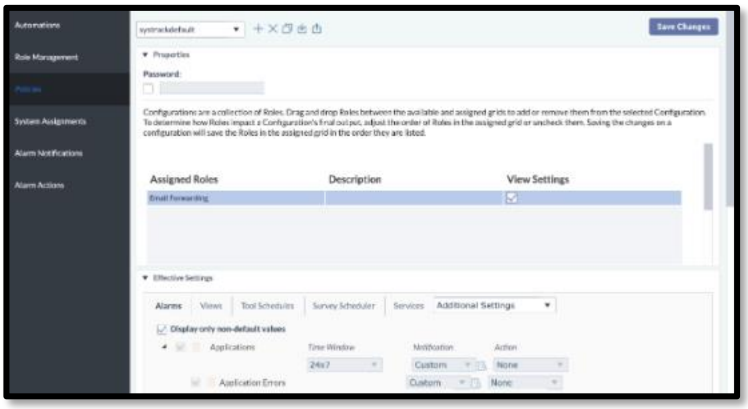
When Email forwarding role is imported and configured, it is necessary to assign that role.

To assign the email forwarding role:

13. Select the **Configurations** page, select **systrackdefault** in the drop-down list.

IMPORTANT LDI Plus by default assigns systrackdefault to all machines in System Assignments and this configuration includes many recommended features. When you create new automation configurations, we recommend you duplicate the systrackdefault policy and apply your policy changes to the duplicate systrackdefault plus so that your devices with new configurations are consistent with the default features.

14. Search for the Email Forwarding role from the list of the available roles.
15. Drag the role to the **Assigned Roles** area.
16. To verify that everything is configured correctly, check all Alarm settings for that role.



Configurations are a collection of Roles. Drag and drop Roles between the available and assigned grids to add or remove them from the selected Configuration. To determine how Roles impact a Configuration's final output, adjust the order of Roles in the assigned grid or uncheck them. Saving the changes on a configuration will save the Roles in the assigned grid in the order they are listed.

Assigned Roles	Description	View Settings
Email Forwarding		☑

☑ Display only non-default values

	Time Window	Notification	Action
Applications	24x7	Custom	None
Application Errors		Custom	None

17. Once everything is set up, read the configuration. To do so, follow these steps:
    - Select the **Administration** page. In the **System Selection** section, select All systems, and select devices that need to be monitored.
    - Click **Read Configuration** and then click **Run**.
    - In the **Command Report** Tab, a Read Configuration with the number of selected devices are displayed under the checkmark.

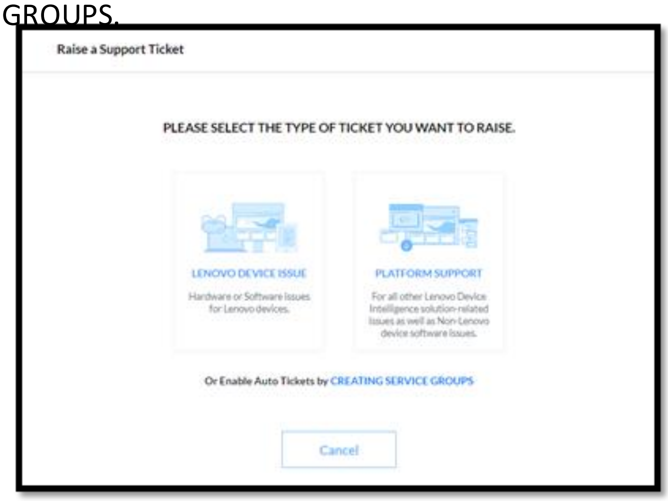
Note: Each time any changes are made, it is important to repeat step 5 and read the configuration if changes are required to be reflected immediately. Otherwise, the system would update within next 24 hours and get the new configuration automatically.

5.10 Involve Lenovo to mitigate hardware issues

A user can create a Service Group by entering information for that group. The system identifies critical issues with any device that is part of that Service Group and automatically create a support ticket.

Create a Service Group

18. Raise a Support Ticket and select Or Enable Auto Tickets by CREATING SERVICE GROUPS.



Raise a Support Ticket

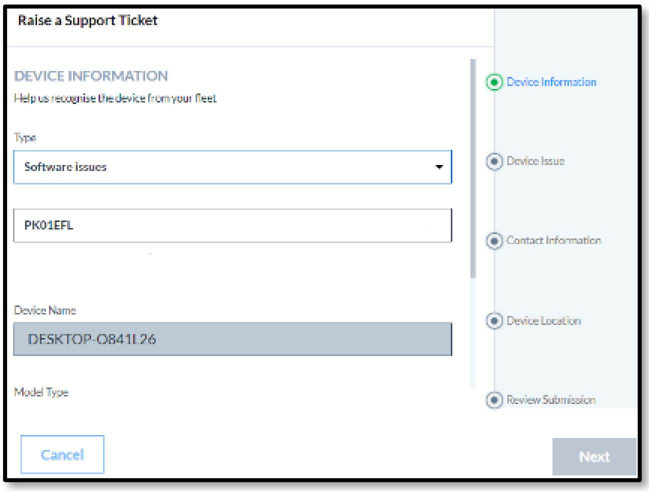
PLEASE SELECT THE TYPE OF TICKET YOU WANT TO RAISE.

LENOVO DEVICE ISSUE
Hardware or Software issues for Lenovo devices.

PLATFORM SUPPORT
For all other Lenovo Device Intelligence solution-related issues as well as Non-Lenovo device software issues.

Or Enable Auto Tickets by CREATING SERVICE GROUPS

2. Complete the information requested.



Raise a Support Ticket

DEVICE INFORMATION
Help us recognise the device from your fleet

Type: Software issues

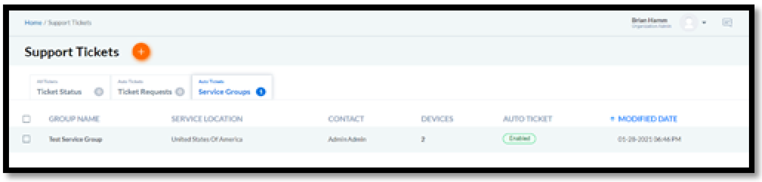
PK01EFL

Device Name: DESKTOP-O841L26

Model Type

- Device Information
- Device Issue
- Contact Information
- Device Location
- Review Submission

3. Once created, the Service Group is displayed on the **Support Tickets** page under the Service Groups tab:

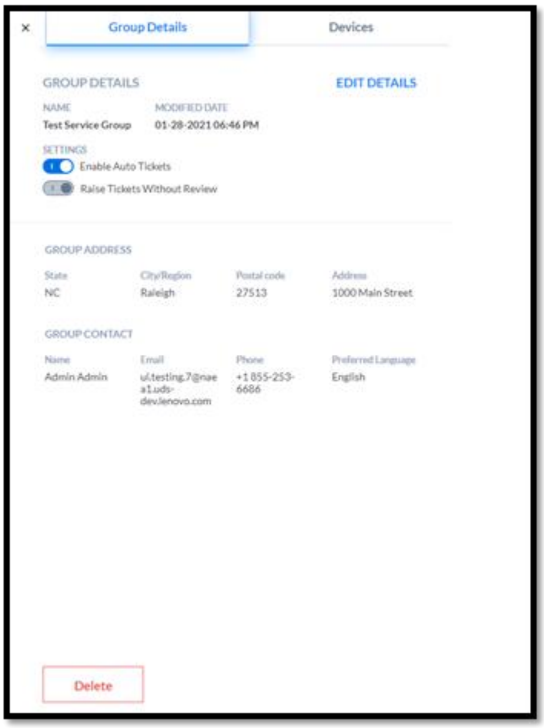


Home / Support Tickets

Support Tickets

GROUP NAME	SERVICE LOCATION	CONTACT	DEVICES	AUTO TICKET	MODIFIED DATE
Test Service Group	United States Of America	Admin Admin	2	Enabled	05-28-2021 06:46 PM

4. View Group Details by selecting the Service Group. You can Enable Auto Tickets and Raise Tickets Without Review.



GROUP DETAILS

NAME	MODIFIED DATE
Test Service Group	01-28-2021 06:46 PM

SETTINGS

Enable Auto Tickets

Raise Tickets Without Review

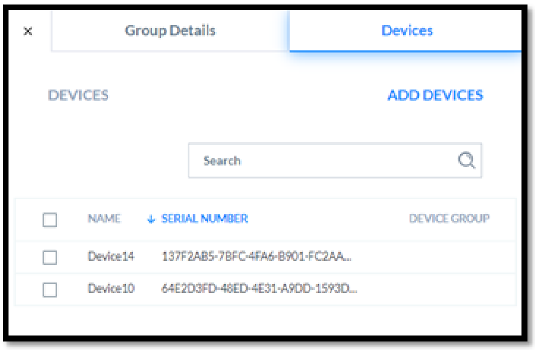
GROUP ADDRESS

State	City/Region	Postal code	Address
NC	Raleigh	27513	1000 Main Street

GROUP CONTACT

Name	Email	Phone	Preferred Language
Admin Admin	ul.testing.7@naea1.uds-dev.lenovo.com	+1 855-253-6686	English

5. Devices assigned to this group may be found under the Devices tab.



DEVICES

☐	NAME	↓ SERIAL NUMBER	DEVICE GROUP
☐	Device14	137F2AB5-7BFC-4FA6-B901-FC2AA...	
☐	Device10	64E2D3FD-48ED-4E31-A9DD-1593D...	

6 Engage End users

6.1 UX Survey

Survey is a useful tool for gathering feedback. IT might want to send a survey to judge the success of an internal initiative, such as rolling out a new piece of software. They might also want to gauge employee sentiment by polling users and other use cases.

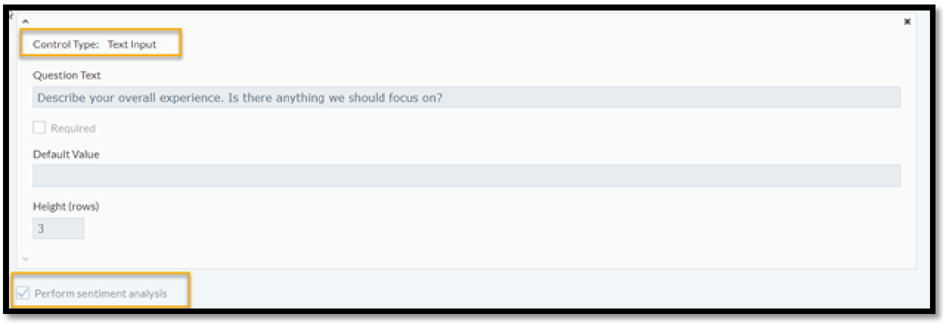
The surveys are flexible and can be used to investigate the characteristics, behaviours, or views of a group of people. If you want quantitative feedback from the users of your fleet, you can gather responses that play an essential role in uncovering latent issues and explaining user behaviour.

Some functionality of surveys may be limited until further releases.

Gathering Sentiment

Using the UX Survey tool, you can gather sentiment about how users feel regarding specific questions. To do this, make sure you do the following:

Note: You must use the text input questions and check the Perform sentiment analysis box. Feedback must include at least three words with positive or negative expression.



Control Type: Text Input

Question Text

Describe your overall experience. Is there anything we should focus on?

□ Required

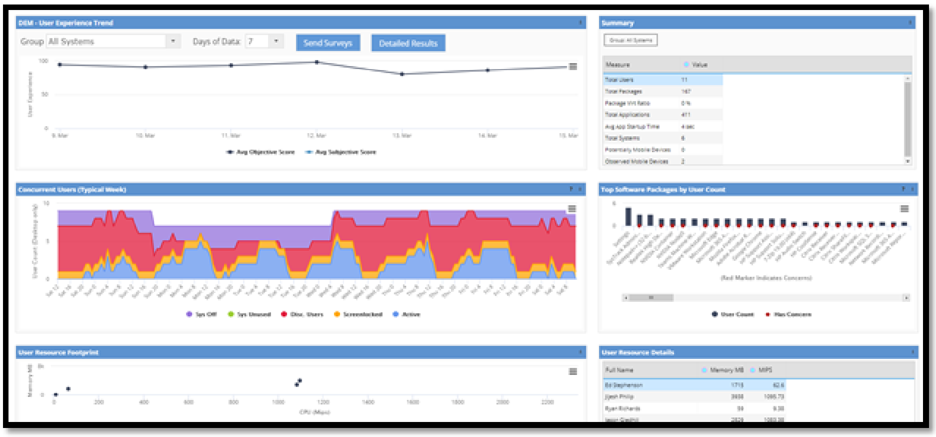
Default Value

Height (rows)

3

☑ Perform sentiment analysis

Once their feedback has been received, a cognitive service analyses and assigns a score to each answer, assigning a positive or negative sentiment. This sentiment is reflected through User Experience scores. You can view this by going to User Experience > Device View > Dashboard.



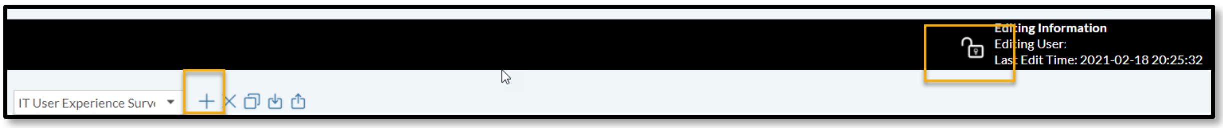
Measure	Value
Total Users	11
Total Packages	167
Package VH Ratio	0 %
Total Applications	471
Avg App Startup Time	4 sec
Total Systems	8
Potentially Mobile Devices	0
Observed Mobile Devices	2

Full Name	Memory MB	MIPS
Ed Stephenson	1713	62.6
Jjesh Philip	3938	1096.73
Ryan Richards	84	8.30
Jason Gledhill	2829	1083.38

6.1.1 Create a Survey

Allows you to build end-user surveys that can be integrated into LDI Plus. The survey appears as a pop-up dialog on the end user's screen.

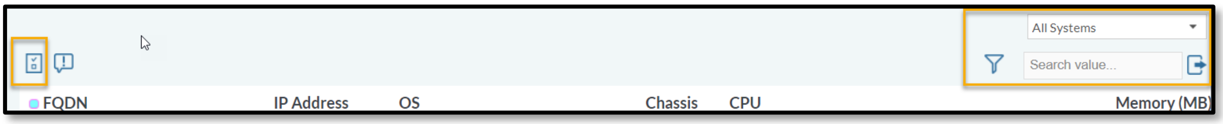
- Click the lock icon in the top right to unlock the page for editing.
- Click the plus + icon on the left to create a new survey.
- Create a name for survey and add an Introduction and Exit text.
- Select **Add Question** to start building your survey.
- Use the different question types to effectively gather information from your users.



6.1.2 Send a Survey

Allows you to send surveys created in Survey Builder by selecting groups or filtering for specific systems.

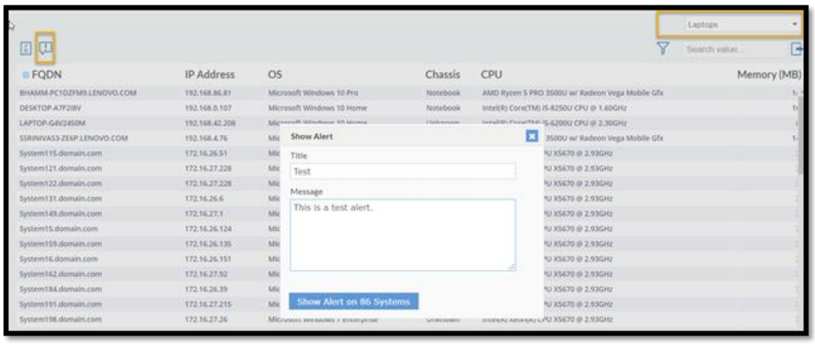
19. Select the Group that you want to survey from the drop-down list in the upper left.
20. Filter for specific systems, if desired.
21. Click the **Show Survey** icon to choose the survey you want users to see.
22. Click **Show Survey on** to send the survey.



6.1.3 Send an Alert

You can use the Send Alert function under Send Survey to push an alert notification to the devices you choose.

23. Select a system or group.
24. Select the exclamation point icon in the upper left.
25. Add text to your alert.
26. Click **Show Alert** on X Systems to send.



FQDN	IP Address	OS	Chassis	CPU	Memory (MB)
BHAMM-PC1DZFM9.LENOVO.COM	192.168.86.81	Microsoft Windows 10 Pro	Notebook	AMD Ryzen 5 PRO 3500U w/ Radeon Vega Mobile Gfx	1-
DESKTOP-A7F2I8V	192.168.0.107	Microsoft Windows 10 Home	Notebook	Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz	1
LAPTOP-G4V2450M	192.168.42.208	Microsoft Windows 10 Home	Unknown	Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz	
SSRINIVAS3-ZE6P.LENOVO.COM	192.168.4.76	Mic		3500U w/ Radeon Vega Mobile Gfx	1-
System115.domain.com	172.16.26.51	Mic		U X5670 @ 2.93GHz	
System121.domain.com	172.16.27.228	Mic		U X5670 @ 2.93GHz	
System122.domain.com	172.16.27.228	Mic		U X5670 @ 2.93GHz	
System131.domain.com	172.16.26.6	Mic		U X5670 @ 2.93GHz	
System149.domain.com	172.16.27.1	Mic		U X5670 @ 2.93GHz	
System15.domain.com	172.16.26.124	Mic		U X5670 @ 2.93GHz	
System159.domain.com	172.16.26.135	Mic		U X5670 @ 2.93GHz	
System16.domain.com	172.16.26.151	Mic		U X5670 @ 2.93GHz	
System162.domain.com	172.16.27.92	Mic		U X5670 @ 2.93GHz	
System184.domain.com	172.16.26.39	Mic		U X5670 @ 2.93GHz	
System191.domain.com	172.16.27.215	Mic		U X5670 @ 2.93GHz	
System198.domain.com	172.16.27.26	Microsoft Windows 7 Enterprise	Unknown	Intel(R) Xeon(R) CPU X5670 @ 2.93GHz	

Show Alert

Title: Test

Message: This is a test alert.

Show Alert on 86 Systems

7 Integrate with Outside Systems

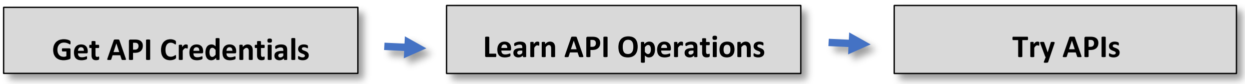
7.1 RESTful API

7.2 Purpose

The purpose of this guide is to inform you how to generate API credentials from your organization admin account, authenticate APIs and use them to integrate LDI with external platforms or applications.

7.3 Audience

This guide is for IT Administrators, Managers, and Developers.



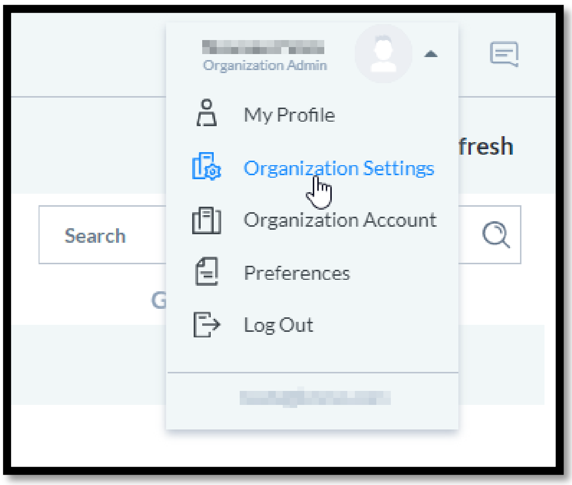
Get API Credentials → **Learn API Operations** → **Try APIs**

7.4 Get API Credentials

> **Note**: You must have an Organization Administration account in LDI portal to generate API credentials.

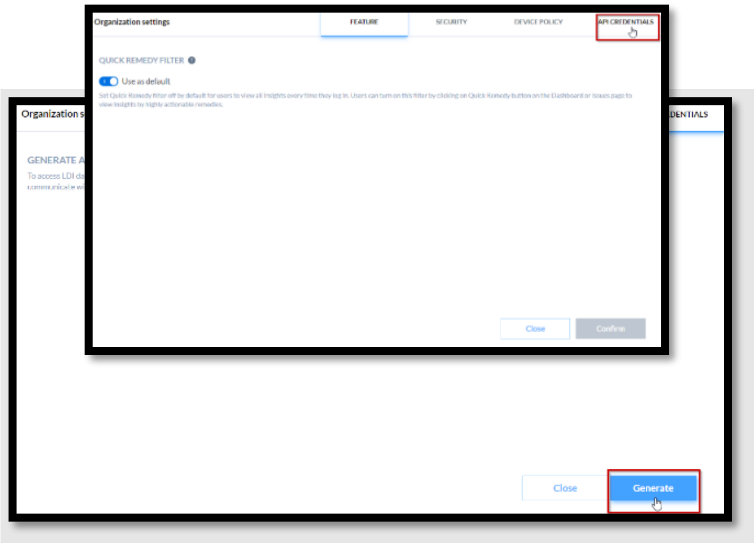
Before you use LDI APIs, you must generate API credentials in the LDI account.

1. Click **Organization Settings** in the Users drop-down list.



2. Click **API Credentials**. You see API Credentials pane.

Note: If there are no API credentials, you must generate them.



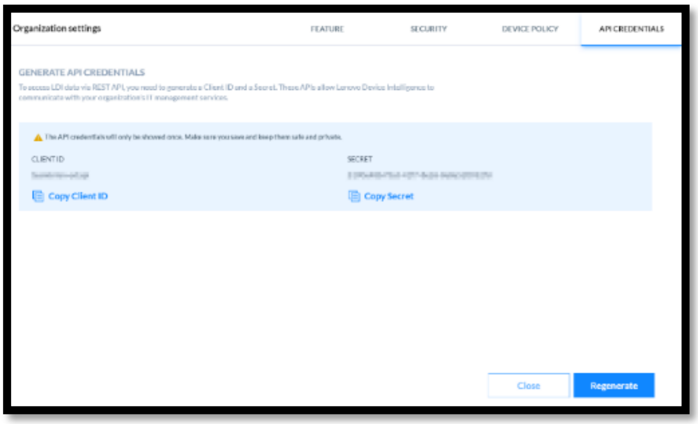
Set Quick Remedy filter off by default for users to view all insights every time they log in. Users can turn on this filter by clicking on Quick Remedy button on the Dashboard or Issues page to view insights by highly actionable remedies.

Note: A Client ID and Secret key are generated. You can copy them to the clipboard.

WARNING ⚠ **Keep the API credentials in a secure place and regenerate them over the time in accordance with business policies of your organization.**

If you want to change the existing API credentials, you must generate a new one.

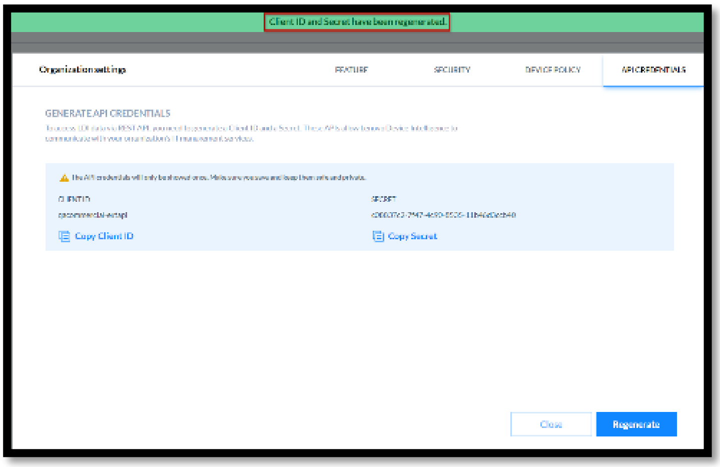
4. Click **Regenerate**.



To access LDI data via REST API, you need to generate a Client ID and a Secret. These APIs allow Lenovo Device Intelligence to communicate with your organization's IT management services.

The API credentials will only be showed once. Make sure you save and keep them safe and private.

5. In the **Regenerate Secret** window, click **Regenerate**.
6. A new Client ID and Secret key is generated.


Client ID and Secret have been regenerated.

GENERATE API CREDENTIALS

To access LDI data via REST API, you need to generate a Client ID and a Secret. These APIs allow Lenovo Device Intelligence to communicate with your organization's IT management services.

The API credentials will only be showed once. Make sure you save and keep them safe and private.

CLIENT ID
qacommercial-extapi

SECRET
c06037c3-7947-4c90-8526-11b46a0acb40

The Client ID and Secret key do not expire until you regenerate a fresh pair.

After you have generated API credentials, you can use the following URLs to access different API endpoints.

Type the URL : https://auth.naea1.uds.lenovo.com or https://auth.euwe1.uds.lenovo.com, depending upon the organization region the devices are located.

Generate LDI API credentials (Client ID and Secret).

LDI API URLs

1. NA

External API: https://api.naea1.uds.lenovo.com
Authentication: https://auth.naea1.uds.lenovo.com

2. EU

External API: https://api.euwe1.uds.lenovo.com
Authentication: https://auth.euwe1.uds.lenovo.com

NA is North American Region and EU is European Union Region.

Note: After you generate a new pair of Client ID and Secret key, the older pair gets invalid.

The bearer token is a type of an access token that uses Auth 2.0 and expires within 30 minutes. You use the bearer token to get a new Access token. To get an access token you send the Authentication server this bearer token along with your client id. This way the server knows that the application using the bearer token is the same application that the bearer token was created for.

Generate API bearer token using External API.

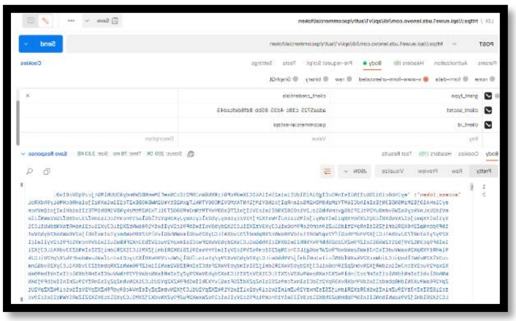
The URL - Base URL + /api/v1/auth/<organization_name>/token

Note: The Base URL depends on your region whether NA or EU.

Body should be x-ww-form-urlencoded and should contain:

- grant_type: client_credentials
- client_secret: secret (from api credentials page)
- client_id: id (from api credentials page)

Note: Generate a new bearer token when it expires after 30 minutes.

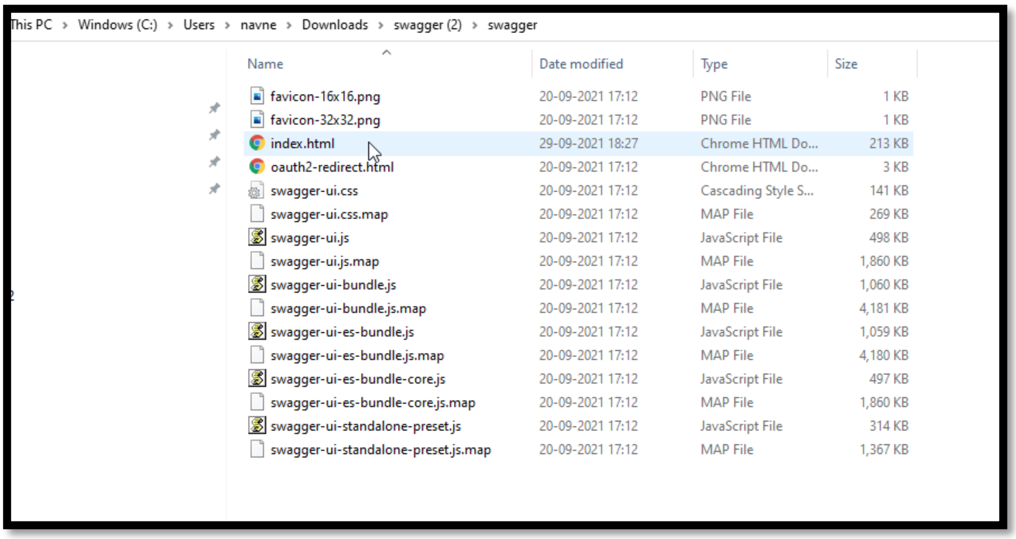


```
private synchronized Tuple2<String, Instant> fetchNewToken() {
    Instant now = Instant.now();
    var response = authClient
            .POST_FORM("/api/v1/auth/" + realm + "/token",
                    Map.of("grant_type", "client_credentials",
                            "client_id", clientId,
                            "client_secret", clientSecret));
    if (response.code >= 400) throw new RuntimeException("Token not
retrieved: " + response.asString());
    var body = response.asMap();
    String accessToken = (String) body.get("access_token");
    int expiredIn = ((Number) body.get("expires_in")).intValue();
    return new Tuple2<>(accessToken, now.plusSeconds(expiredIn - 15));
}
 public synchronized String getToken() {
    if ((token == null) || (token.getV2().isAfter(Instant.now())))
```

7.5 Learn API Operations

Swagger specification archive contains a folder with an index.html file and some other JavaScript files.

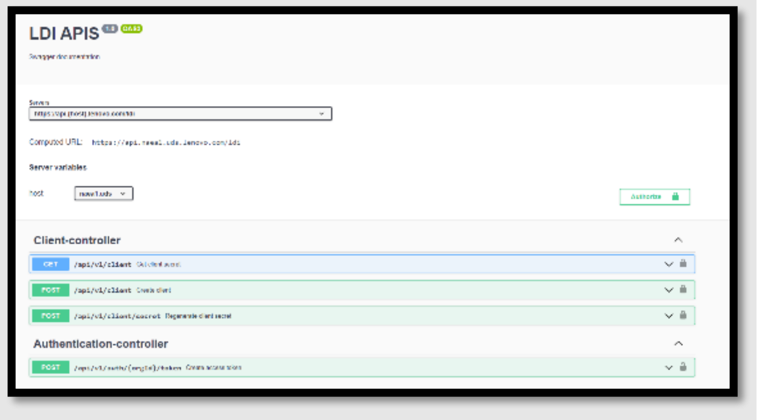
1. Download Swagger Specification zip file from the **support site** which provides you details about each API.
2. Extract the files in the folder.



This PC › Windows (C:) › Users › navne › Downloads › swagger (2) › swagger

Name	Date modified	Type	Size
favicon-16x16.png	20-09-2021 17:12	PNG File	1 KB
favicon-32x32.png	20-09-2021 17:12	PNG File	1 KB
index.html	29-09-2021 18:27	Chrome HTML Do...	213 KB
oauth2-redirect.html	20-09-2021 17:12	Chrome HTML Do...	3 KB
swagger-ui.css	20-09-2021 17:12	Cascading Style S...	141 KB
swagger-ui.css.map	20-09-2021 17:12	MAP File	269 KB
swagger-ui.js	20-09-2021 17:12	JavaScript File	498 KB
swagger-ui.js.map	20-09-2021 17:12	MAP File	1,860 KB
swagger-ui-bundle.js	20-09-2021 17:12	JavaScript File	1,060 KB
swagger-ui-bundle.js.map	20-09-2021 17:12	MAP File	4,181 KB
swagger-ui-es-bundle.js	20-09-2021 17:12	JavaScript File	1,059 KB
swagger-ui-es-bundle.js.map	20-09-2021 17:12	MAP File	4,180 KB
swagger-ui-es-bundle-core.js	20-09-2021 17:12	JavaScript File	497 KB
swagger-ui-es-bundle-core.js.map	20-09-2021 17:12	MAP File	1,860 KB
swagger-ui-standalone-preset.js	20-09-2021 17:12	JavaScript File	314 KB
swagger-ui-standalone-preset.js.map	20-09-2021 17:12	MAP File	1,367 KB

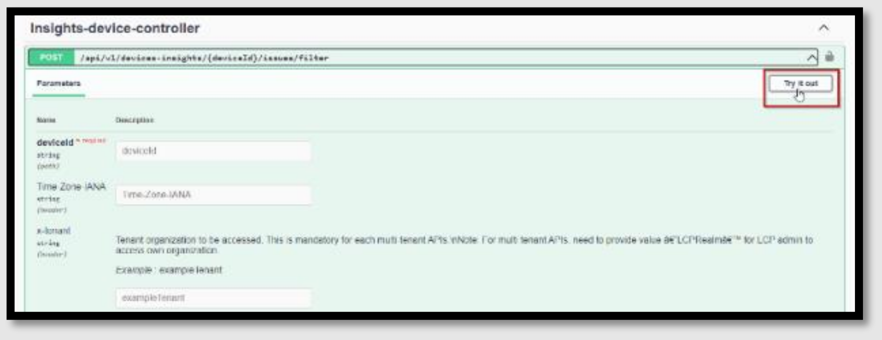
3. Double-click to open the index.html. You see the LDI APIs home page in Swagger.



4. Generate a bearer token (Refer Get API Credentials and Postman example).

7.6 Try APIs

1. Select an API method in Swagger.



Insights-device-controller

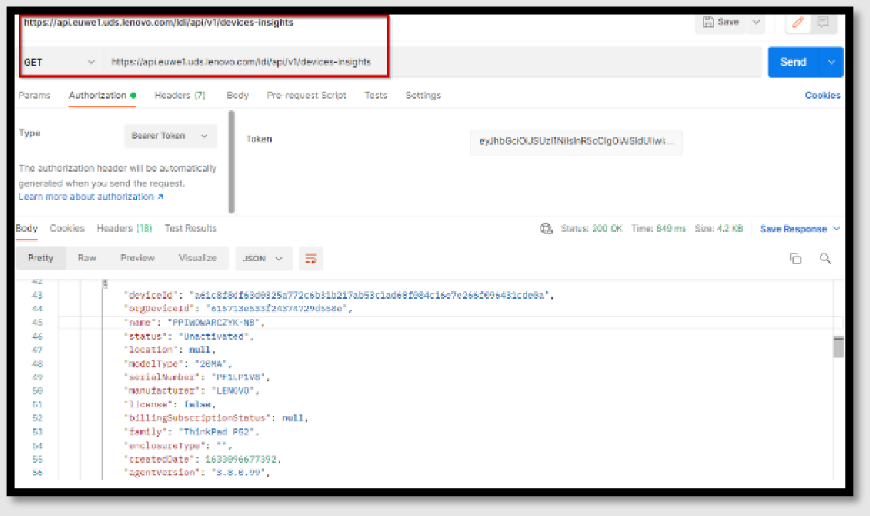
POST /api/v1/devices-insights/{deviceId}/issues/filter

Parameters

Try it out

Name	Description
deviceId * required string (path)	deviceId
Time Zone IANA string (header)	Time-Zone-IANA
x-tenant string (header)	Tenant organization to be accessed. This is mandatory for each multi tenant APIs \nNote: For multi tenant APIs, need to provide value â€˜LCPRealmâ€™ for LCP admin to access own organization Example : example tenant exampleTenant

2. Use the bearer token in the call.
3. Click Try it out.



https://api.euwe1.uds.lenovo.com/ldi/api/v1/devices-insights

GET https://api.euwe1.uds.lenovo.com/ldi/api/v1/devices-insights

Type: Bearer Token

Token: eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwi...

The authorization header will be automatically generated when you send the request.
Learn more about authorization ↗

Status: 200 OK Time: 849 ms Size: 4.2 KB

```
        "deviceId": "a61c8f8df63d0325a772c6b31b217ab53c1ade8f084c16e7e266d696431cde8a",
        "orgDeviceId": "615713e533f24374729d558e",
        "name": "PPIWOWARCZYK-NB",
        "status": "Unactivated",
        "location": null,
        "modelType": "20MA",
        "serialNumber": "PF1LP1V8",
        "manufacturer": "LENOVO",
        "license": false,
        "billingSubscriptionStatus": null,
        "family": "ThinkPad P52",
        "enclosureType": "",
        "createdDate": 1633096677392,
        "agentVersion": "3.3.0.99",
```

7.7 Examples of API Methods

7.7.1.1. Authentication - API token session

```
ACME JAVA CODE
package com.acme.ldi.test;
public class LdiClientTest {
    @org.junit.Test
    void tokenTest() {
        // parameters depends on geography
        String authUrl = "https://api.uds-qa.lenovo.com";
        String apiUrl = "https://api.uds-qa.lenovo.com";
        // realm name supplied by sales team
        String realm = "autoticketing";
        // client id to be supplied by integration support team
        String clientId = "autoticketing-extapi";
        // client secret gotten via UI self-service
        String clientSecret = "0bf4c041-a9b1-4133-9045-73795a254439";
```

Lenovo SDK snapshot

```
POST https://api.uds-qa.lenovo.com/ldi/api/v1/auth/autoticketing/token
Content-Type: application/x-www-form-urlencoded

client_id=autoticketing-extapi&client_secret=0bf4c041-a9b1-4133-9045-
73795a254439&grant_type=client_credentials
```

```
private synchronized Tuple2<String, Instant> fetchNewToken() {
    Instant now = Instant.now();
    var response = apiClient
            .POST_FORM("/ldi/api/v1/auth/" + realm + "/token",
                    Map.of("grant_type", "client_credentials",
                            "client_id", clientId,
                            "client_secret", clientSecret));
    if (response.code >= 400) throw new RuntimeException("Token not
retrieved: " + response.asString());
    var body = response.asMap();
    String accessToken = (String) body.get("access_token");
    int expiredIn = ((Number) body.get("expires_in")).intValue();
    return new Tuple2<>(accessToken, now.plusSeconds(expiredIn - 15));
}
 public synchronized String getToken() {
    if ((token == null) || (token.getV2().isAfter(Instant.now())))
        token = fetchNewToken();
    return token.getV1();
```

```
date: Tue, 28 Sep 2021 11:47:12 GMT

pragma: no-cache

referrer-policy: no-referrer

server: Lenovo

set-cookie: KC_RESTART=; Version=1; Expires=Thu, 01-Jan-1970 00:00:10 GMT;
Max-Age=0; Path=/auth/realms/autoticketing/; Secure; HttpOnly

strict-transport-security: max-age=31536000; includeSubDomains

x-content-type-options: nosniff

x-frame-options: SAMEORIGIN

x-xss-protection: 1; mode=block

 {"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJwZG1iME41
R

….(truncated text)

zU0Nk1CX0RBOFJUOyKRZ-H716fnlFWk54eCn2vouFmKFz2frAuR9kE-
bgp3AhTSOuT6nlb4HGmSrMNNkYbg","expires_in":15552000,"refresh_expires_in":0,"to
ken_type":"Bearer","not-before-policy":0,"scope":"email profile"}
```

7.8 Negative API Sample

7.8.1.1. Groovy ACME Test

```
@Test
    void tokenNegativeTest() {
        var client = new com.lenovo.ldi.client.LdiClient(authUrl, apiUrl, realm,
clientId, clientSecret + "_INVALID");
        var response = client.authClient
                .POST_FORM("/auth/realms/" + realm + "/protocol/openid-
connect/token",
                        [grant_type   : "client_credentials",
                         client_id    : clientId,
                         client_secret: clientSecret])
        assert response.code == 401
```

```
POST https://auth.uds-qa.lenovo.com/auth/realms/autoticketing/protocol/openid-
connect/token

Content-Type: application/x-www-form-urlencoded


grant_type=client_credentials&client_secret=0bf4c041-a9b1-4133-9045-
73795a254439-INVALID&client_id=autoticketing-extapi
```

HTTP Response

```
401
access-control-allow-credentials: true
cache-control: no-store
content-length: 75
content-security-policy: frame-src 'self'; frame-
ancestors 'self' https://portal.uds-
qa.lenovo.com https://developer.naea1.uds-qa.lenovo.com; object-src 'none';
content-type: application/json
date: Tue, 28 Sep 2021 13:29:06 GMT
pragma: no-cache
referrer-policy: no-referrer
server: Lenovo
strict-transport-security: max-age=31536000; includeSubDomains
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
```

7.9 User Management

```
package com.acme.ldi.test
import org.junit.jupiter.api.Test
class UserTests extends BaseLdiTestClass {
    @Test
    void createNewUser() {
        var response =
this.client.authenticatedRestConnector.POST("/ldi/api/v1/users",
                [loginId          : "ccretoiu@lenovo.com",
                 compositeRoleName: "pm_org_admin",
                 firstName        : "ABC",
                 creatorId        : "autoticketing",
                 country          : "USA",
                 email            : "ccretoiu@lenovo.com",
                 lastName         : "ABC"])
        assert response.code == 409 // Expected conflict
    }
    @Test
    void getAllUsers() {
        var response =
this.client.authenticatedRestConnector.GET("/ldi/api/v1/users")
        assert response.code == 200
        var body = response.asMap()
        assert body.keySet() == ['_embedded', 'page', 'responseType'] as Set
        var usersList = body._embedded.userList
        var loginIds = usersList*.loginId
        println "${loginIds.size()} users found: ${loginIds}"
    }
    @Test
    void createAndDeleteUser() {
        var seed = Math.random().toString().replaceAll(/[^\d]/, '')
        var response =
this.client.authenticatedRestConnector.POST("/ldi/api/v1/users",
                [loginId          : "sdragos.${seed}@lenovo.com",
                 compositeRoleName: "pm_org_admin",
                 firstName        : "ABC",
                 creatorId        : "autoticketing",
                 country          : "USA",
                 email            : "sdragos.${seed}@lenovo.com",
                 lastName         : "ABC"])
        assert response.code == 201
        var searchResult =
this.client.authenticatedRestConnector.GET("/ldi/api/v1/users",
[freeText: "sdragos.${seed}@lenovo.com"])
        assert searchResult.asMap()._embedded.userList*.loginId ==
["sdragos.${seed}@lenovo.com"]
        var userDetails = searchResult.asMap()._embedded.userList[0]

        var deleteResponse =
this.client.authenticatedRestConnector.PATCH("/ldi/api/v1/users",
                ["userList" : [userDetails.userId],
                 "operation": "DELETE"]
        )
        var secondSearchResult =
this.client.authenticatedRestConnector.GET("/ldi/api/v1/users",
[freeText: "sdragos.${seed}@lenovo.com"])
        var usersList=secondSearchResult.asMap()?._embedded?.userList
        assert (usersList?.collect { it['loginId'] } ?: []).empty
    }
}
```

7.9.1 GET Users

HTTP Request

```
GET https://api.uds-qa.lenovo.com/ldi/api/v1/users

Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJwZG1iME41RzU0Nk1CX0RBOFJUOW
… (truncated text)  vxilXFgr4gKVbCfnnVUScQXPkcGF2aqifGEQNaLiIXsBWM8iAX8smq-
2YNZdY509LuBw
```

API Response

```
200
cache-control: no-cache, no-store, max-age=0, must-revalidate
content-security-policy: default-src 'self'; connect-src *.uds-qa.lenovo.com;
style-src 'self' 'unsafe-inline'; img-src 'self' data:; script-
src 'self' 'unsafe-inline'; object-src 'none';
content-type: application/json
date: Wed, 29 Sep 2021 10:31:13 GMT
expires: 0
pragma: no-cache
referrer-policy: no-referrer
server: Lenovo
strict-transport-security: max-age=31536000; includeSubDomains
transfer-encoding: chunked
x-content-type-options: nosniff
x-envoy-upstream-service-time: 349
x-frame-options: DENY
x-xss-protection: 1; mode=block


{"_embedded":{"userList":[{"userId":"7204a566-1495-4be8-8c76-19899adf508d"…
(truncated
text)…{"number":0,"size":8,"totalElements":8,"totalPages":1},"responseType":"P
AGE"}
```

Stdout

```
8 users found: [shuma@lenovo.com, sdragos@lenovo.com, penghong2@lenovo.com,
penghong221062911034172@lenovo.com, penghong2+21063007144784@lenovo.com,
otsiupa@lenovo.com, ccretoiu@lenovo.com, ladamestean1@lenovo.com]
```

7.9.2 Create User

```
POST https://api.uds-qa.lenovo.com/ldi/api/v1/users
```

```
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJwZG1iME41RzU0Nk1CX0RBOFJUOW
…(truncated text)…. -4NQ

Content-Type: application/json; charset=utf-8

{

    "loginId": "ccretoiu@lenovo.com",

    "compositeRoleName": "pm_org_admin",

    "firstName": "ABC",

    "creatorId": "autoticketing",

    "country": "USA",

    "email": "ccretoiu@lenovo.com",

    "lastName": "ABC"
}
```

```
409

cache-control: no-cache, no-store, max-age=0, must-revalidate

content-length: 99

content-security-policy: default-src 'self'; connect-src *.uds-qa.lenovo.com;
style-src 'self' 'unsafe-inline'; img-src 'self' data:; script-
src 'self' 'unsafe-inline'; object-src 'none';

content-type: application/json

date: Wed, 29 Sep 2021 10:31:15 GMT

expires: 0

pragma: no-cache

referrer-policy: no-referrer

server: Lenovo

strict-transport-security: max-age=31536000; includeSubDomains

x-content-type-options: nosniff
```

```
x-envoy-upstream-service-time: 54
x-frame-options: DENY
x-xss-protection: 1; mode=block
{"messages":["User with login id ccretoiu@lenovo.com already exist in
organization autoticketing"]}
```

Email

```
GET https://api.uds-
qa.lenovo.com/ldi/api/v1/users?freeText=sdragos.02879781611736808%40lenovo.com
```

```
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJwZG1iME41RzU0Nk1CX0RBOFJUOW
…(truncated text)… SMHqjNONc5SeugT5C4dINKENr0Mlh933i6qw
```

```
200
cache-control: no-cache, no-store, max-age=0, must-revalidate
content-length: 1269
content-security-policy: default-src 'self'; connect-src *.uds-qa.lenovo.com;
style-src 'self' 'unsafe-inline'; img-src 'self' data:; script-
src 'self' 'unsafe-inline'; object-src 'none';
content-type: application/json
date: Wed, 29 Sep 2021 10:31:18 GMT
expires: 0
pragma: no-cache
referrer-policy: no-referrer
server: Lenovo
strict-transport-security: max-age=31536000; includeSubDomains
x-content-type-options: nosniff
x-envoy-upstream-service-time: 183
x-frame-options: DENY
x-xss-protection: 1; mode=block
{"_embedded":{"userList":[{"userId":"555fcf91-9dca-4fc6-9df5-…(truncated
text)…number":0,"size":1,"totalElements":1,"totalPages":1},"responseType":"PAG
E"}
```

7.9.3 Delete User

```
PATCH https://api.uds-qa.lenovo.com/ldi/api/v1/users
```

```
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJwZG1iME41RzU0Nk1CX0RBOFJUOW
…(truncated text)… KBLeWSCisibDjTmr8RNt4w
Content-Type: application/json; charset=utf-8
{
    "userList": [
        "555fcf91-9dca-4fc6-9df5-4d9f38841e2d"
    ],
    "operation": "DELETE"
}
```

```
200
cache-control: no-cache, no-store, max-age=0, must-revalidate
content-length: 95
content-security-policy: default-src 'self'; connect-src *.uds-qa.lenovo.com;
style-src 'self' 'unsafe-inline'; img-src 'self' data:; script-
src 'self' 'unsafe-inline'; object-src 'none';
content-type: application/json
date: Wed, 29 Sep 2021 10:31:20 GMT
expires: 0
pragma: no-cache
referrer-policy: no-referrer
server: Lenovo
strict-transport-security: max-age=31536000; includeSubDomains
x-content-type-options: nosniff
x-envoy-upstream-service-time: 601
x-frame-options: DENY
x-xss-protection: 1; mode=block
{"operationSuccessfulUsers":["555fcf91-9dca-4fc6-9df5-
4d9f38841e2d"],"operationFailedUsers":[]}
```

7.10 Devices

7.10.1.1. ACME Client Code

Acme Groovy Code

```
package com.acme.ldi.test
 import org.junit.jupiter.api.Test
```

```
class DevicesTests extends BaseLdiTestClass {
    @Test
    void getDevices() {
        var response =
client.authenticatedRestConnector.GET("/ldi/api/v1/devices/")
        assert response.code == 200
         var body = response.asMap()
        assert body.keySet() ==
['content', 'pageable', 'last', 'totalElements', 'totalPages', 'sort', 'first'
, 'number', 'numberOfElements', 'size', 'empty'] as Set
        assert body['content'] instanceof List
    }
     @Test
    void export() {
        var deviceId =
client.authenticatedRestConnector.GET("/ldi/api/v1/devices/").asMap()['content
'][0]['deviceId']
        var response =
client.authenticatedRestConnector.POST("/ldi/api/v1/devices/bulk/export",
                [ids: [deviceId]])
        assert response.code == 200
        var file = response.asFile()
        assert file.name =~ /.*.csv/
        assert file.text.split(/\v/)[0] == 'DEVICE NAME,MACHINE TYPE,SERIAL
NUMBER,GROUP'
    }
}
```

7.10.1.2. HTTP Request Responses

Get Devices

Request

```
GET https://api.uds-qa.lenovo.com/ldi/api/v1/devices/
```

```
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJwZG1iME41RzU0Nk1CX0RBOFJUOW
…(truncated text)…N0LFHsvE7Q09QXeGzoU0IS86PlDFl6BhEEcXzN5Pow
```

```
200
cache-control: no-cache, no-store, max-age=0, must-revalidate
```

```
content-security-policy: default-src 'self'; connect-src *.uds-qa.lenovo.com; 
style-src 'self' 'unsafe-inline'; img-src 'self' data:; script-
src 'self' 'unsafe-inline'; object-src 'none';
content-type: application/json
date: Tue, 28 Sep 2021 15:37:56 GMT
expires: 0
pragma: no-cache
referrer-policy: no-referrer
server: Lenovo
strict-transport-security: max-age=31536000; includeSubDomains
transfer-encoding: chunked
x-content-type-options: nosniff
x-envoy-upstream-service-time: 543
x-frame-options: DENY
x-xss-protection: 1; mode=block
 {"content":[{"orgDeviceId":"6112d2990e9e6a202b99effc","deviceId":""},"orgId":
…(truncated 
text)…{"sorted":true,"unsorted":false,"empty":false},"number":0,"first":true,"
numberOfElements":20,"size":20,"empty":false}
```

7.11 Fleet Management

ACME Code

Fleet Status

```
package com.acme.ldi.test
 import org.junit.jupiter.api.Test
 class FleetManagement extends BaseLdiTestClass {
    @Test
    void fleetStatus() {
        var response = 
client.authenticatedRestConnector.GET("/ldi/api/v1/fleethealth")
        assert response.asMap().keySet() == 
["latestJobRuntime", "timestamp", "fleetHealthScore", "fleetBsodScore", "fleet
StorageScore", "fleetBatteryScore", "fleetWdmScore", "fleetPerformanceScore"] 
as Set
    }
}
```

7.12 Insights Tests

```
package com.acme.ldi.test


import org.junit.jupiter.api.Test
 class InsightsTests extends BaseLdiTestClass {
    @Test
    void insightsTest() {
        var devices =
client.authenticatedRestConnector.GET('/ldi/api/v1/devices').asMap().content
        var deviceId = devices[0].deviceId
        var response =
client.authenticatedRestConnector.POST("/ldi/api/v1/devices-
insights/$deviceId/issues/filter", [:])
        var body = response.asMap()
         assert body.keySet() ==
['content', 'pageable', 'last', 'totalElements', 'totalPages', 'sort', 'first'
, 'number', 'numberOfElements', 'size', 'empty'] as Set
        assert body['size'] == 20
    }
}
```

7.12.1.1. Request

```
GET https://api.uds-qa.lenovo.com/ldi/api/v1/fleethealth
```

```
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJwZG1iME41RzU0Nk1CX0RBOFJUOW
…(truncated
text)…SWWahdAVe1lOwYgQRmbPNnDEoAq_ajmCyTPdDb3SRR2C1JqIjF0za2Yr796vj5xgoyycLOLl
4ydadQ
```

Response

```
200
cache-control: no-cache, no-store, max-age=0, must-revalidate
content-length: 223
content-type: application/json
date: Wed, 29 Sep 2021 10:30:58 GMT
expires: 0
pragma: no-cache
```

```
server: Lenovo
strict-transport-security: max-age=31536000 ; includeSubDomains
x-content-type-options: nosniff
x-envoy-upstream-service-time: 314
x-frame-options: DENY
x-xss-protection: 1; mode=block

{"latestJobRuntime":"2021-09-24T07:49:42.196","timestamp":"2021-09-
10T05:06:01.585638","fleetHealthScore":98,"fleetBsodScore":100,"fleetStorageSc
ore":91,"fleetBatteryScore":94,"fleetWdmScore":99,"fleetPerformanceScore":100}
```

7.13 Issues Filter

Issues Tests

```
package com.acme.ldi.test
 import org.junit.jupiter.api.Test
 class IssuesFilter extends BaseLdiTestClass {
    @Test
    void filterIssues() {
        var response =
client.authenticatedRestConnector.POST('/ldi/api/v1/issues/filter')
        assert response.code == 200
        var body = response.asMap()
         assert body.keySet() ==
['content', 'pageable', 'last', 'totalElements', 'totalPages', 'sort', 'number
', 'first', 'numberOfElements', 'size', 'empty'] as Set
        assert body['pageable']['pageNumber'] == 0
        assert body['pageable']['pageSize'] == 20
        assert body['content'] instanceof List
        println "Found ${body['content'].size()} issues."
    }
     @Test
    void markIssueAsResolved() {
        var response =
client.authenticatedRestConnector.POST('/ldi/api/v1/issues/mark-as-resolved',
                ["issuesUuids": ["fake-issue-uuid"],
                 "comment"    : "Would like to resolve an issue that does NOT
exist."
```

```
                ])
        assert response.code == 404
    }
}
```

Request

```
POST https://api.uds-qa.lenovo.com/ldi/api/v1/issues/filter
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJwZG1iME41RzU0Nk1CX0RBOFJUOW
…(truncated text)…
bzhfSJCvsw8pTti6yVbvHLJVaw1eNkqVkVXJ2DXwDMoAyibXc7OCUmLX0JfH2fU9tfERhYWwd7A
```

Response

```
200
cache-control: no-cache, no-store, max-age=0, must-revalidate
content-type: application/json
date: Wed, 29 Sep 2021 10:31:07 GMT
expires: 0
pragma: no-cache
server: Lenovo
strict-transport-security: max-age=31536000 ; includeSubDomains
transfer-encoding: chunked
x-content-type-options: nosniff
x-envoy-upstream-service-time: 2066
x-frame-options: DENY
x-xss-protection: 1; mode=block
 {"content":[{"bucketId":"app_performance_impact","category":"Excel.exe","code
":null…(truncated text)…
2,"first":true,"numberOfElements":20,"size":20,"empty":false}
```

7.14 Mark Issue as Resolved

```
@Test
void markIssueAsResolved() {
    var response =
client.authenticatedRestConnector.POST('/ldi/api/v1/issues/mark-as-resolved',
            ["issuesUuids": ["fake-issue-uuid"],
             "comment"    : "Would like to resolve an issue that does NOT
exist."
            ])
    assert response.code == 404
}
```

Request

```
POST https://api.uds-qa.lenovo.com/ldi/api/v1/issues/mark-as-resolved
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJwZG1iME41RzU0Nk1CX0RBOFJUOW
…(truncated text)…
_ZD3p_pmiikTMzOJyQQ64CDSxE7DmRjS_zirs0XAnDQ5nIm716XVxn9bqgCriHNoqSERg8CyRWJixL
BRPIe1P5K6Zd184A
Content-Type: application/json; charset=utf-8
 {
    "issuesUuids": [
        "fake-issue-uuid"
    ],
    "comment": "Would like to resolve an issue that does NOT exist."
}
 400
cache-control: no-cache, no-store, max-age=0, must-revalidate
content-length: 1355
content-type: application/json
date: Wed, 29 Sep 2021 10:31:03 GMT
expires: 0
pragma: no-cache
server: Lenovo
strict-transport-security: max-age=31536000 ; includeSubDomains
x-content-type-options: nosniff
x-envoy-upstream-service-time: 71
x-frame-options: DENY
x-xss-protection: 1; mode=block
 {"timestamp":"2021-09-29T10:31:03.761+00:00","status":400,"error":"Bad
Request","message":"400 BAD_REQUEST \"JSON parse error: Cannot deserialize
value of type `java.util.UUID` from String \"fake-issue-uuid\": UUID has to be
represented by standard 36-char representation; nested exception is
com.fasterxml.jackson.databind.exc.InvalidFormatException: Cannot deserialize
value of type `java.util.UUID` from String \"fake-issue-uuid\": UUID has to be
represented by standard 36-char representation\n at [Source:
```

```
(PushbackInputStream); line: 3, column: 9] (through reference chain:
com.lenovo.iss.graphql.rest.request.MarkAsResolvedRequest[\"issuesUuids\"]-
>java.util.HashSet[0])\"","path":"/iss-insights-api/api/issues/mark-as-
resolved","errors":{"defaultMessage":"400 BAD_REQUEST \"JSON parse error:
Cannot deserialize value of type `java.util.UUID` from String \"fake-issue-
uuid\": UUID has to be represented by standard 36-char representation; nested
exception is com.fasterxml.jackson.databind.exc.InvalidFormatException: Cannot
deserialize value of type `java.util.UUID` from String \"fake-issue-uuid\":
UUID has to be represented by standard 36-char representation\n at [Source:
(PushbackInputStream); line: 3, column: 9] (through reference chain:
com.lenovo.iss.graphql.rest.request.MarkAsResolvedRequest[\"issuesUuids\"]-
>java.util.HashSet[0])\""}}
```

Response

```
Assertion failed:
 assert response.code == 404
       |        |    |
       |        400  false
       com.lenovo.ldi.util.RestResponse@f6497e3
     at
org.codehaus.groovy.runtime.InvokerHelper.assertFailed(InvokerHelper.java:436)
    at
org.codehaus.groovy.runtime.ScriptBytecodeAdapter.assertFailed(ScriptBytecodeA
dapter.java:670)
    at
com.acme.ldi.test.IssuesFilter.markIssueAsResolved(IssuesFilter.groovy:25)
    at java.base/java.lang.Thread.run(Thread.java:834)
```

7.15 Sensors

```
package com.acme.ldi.test
 import org.junit.jupiter.api.Test
 class SensorsTest extends BaseLdiTestClass {
    @Test
    void getDefinedSensors() {
        // Test not functional, it's expected to fail
        var response =
client.authenticatedRestConnector.GET("/api/v1/ldiplus/definedsensors?descript
ionApp=1")
        assert response.code == 200 // Test not implemented
    }
   @Test
    void getSensorActions() {
        // Test not functional, it's expected to fail
        var response =
client.authenticatedRestConnector.GET("/api/v1/ldiplus/sensoractions?descriptionApp=1")
        assert response.code == 200 // Test not implemented
    }
}
```

7.16 ServiceNow Integration

The Lenovo Device Intelligence (LDI) Plus ServiceNow Integration Guide helps you setup LDI ServiceNow Plugin so that ServiceNow platform can connect to device(s) in the LDI organization account through LDI external API.

7.16.1 Audience

IT Administrators, Analysts, and Managers.

7.16.2 Prerequisites

- Establish parity between LDI and ServiceNow Platforms.

> **Note**:
> A physical device like laptop, desktop, server, etc. is referred to as a Device in LDI application and as an Asset in the ServiceNow application.

You must synchronize devices in LDI with the Assets or configuration items in the ServiceNow application for the proper working of the LDI ServiceNow plugin. Therefore, you must fulfil the following conditions:

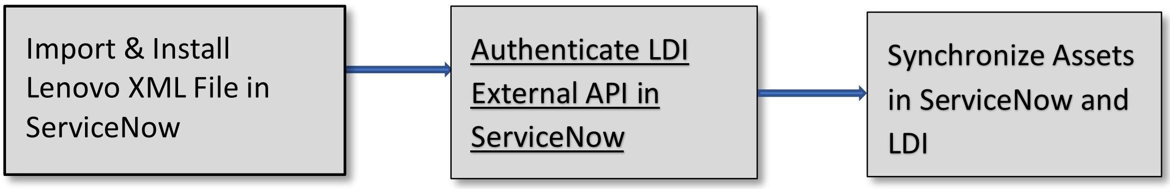
  - The name of the LDI device must be the same as the name of the Asset in the ServiceNow application
  - The Serial number of the LDI device and Asset serial number must be the same.

- Requisite Roles and Rights required for LDI and ServiceNow accounts.

Application	Roles and Rights
Lenovo Device Intelligence (LDI)	You must have an Organization Administrative account to generate API credentials - Client ID and Secret. The API credentials are required for API integration between LDI and

	ServiceNow so that the LDI ServiceNow plugin can work.
ServiceNow	Administrator account

Disclaimer – The LDI ServiceNow plugin was developed and tested in a clear and empty ServiceNow Instance. Any change done by ServiceNow in their platform can affect the LDI ServiceNow plugin.



Import & Install Lenovo XML File in ServiceNow

Authenticate LDI External API in ServiceNow

Synchronize Assets in ServiceNow and LDI

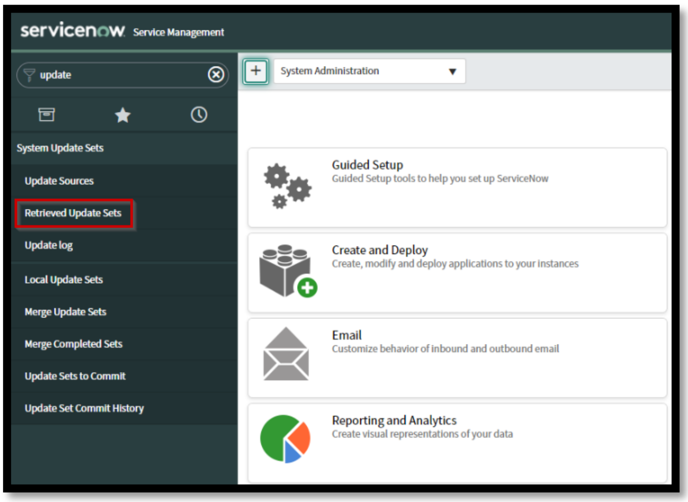
7.16.3 Import and Install Lenovo XML File in ServiceNow

Application Remote Update Set is an XML file that you can import into ServiceNow Instance. The file contains configuration and scripts developed by Lenovo.

Note: It is mandatory to have an administrative account in ServiceNow application.

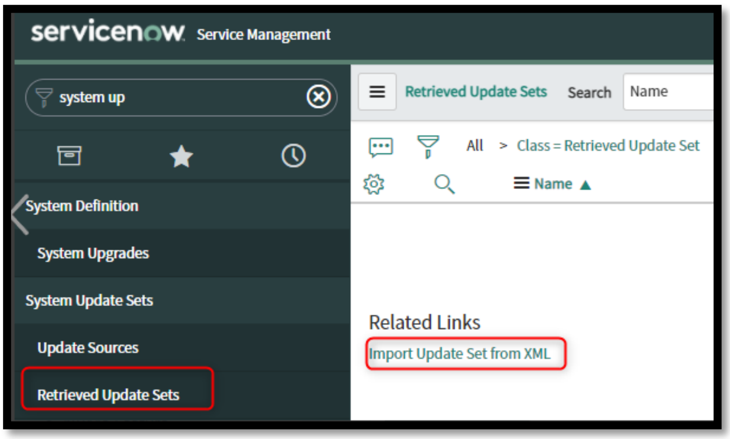
Follow these steps to import and install Lenovo XML file:

1. Sign in to the ServiceNow dashboard.

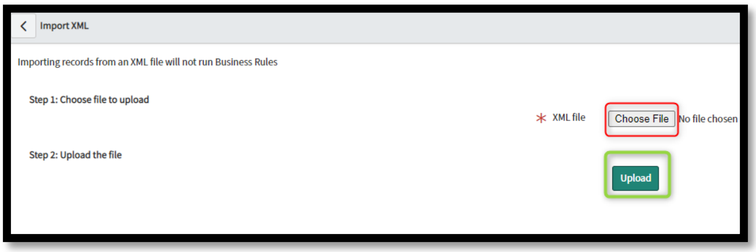


servicenow Service Management
update
System Administration
System Update Sets
Update Sources
Retrieved Update Sets
Update log
Local Update Sets
Merge Update Sets
Merge Completed Sets
Update Sets to Commit
Update Set Commit History
Guided Setup
Guided Setup tools to help you set up ServiceNow
Create and Deploy
Create, modify and deploy applications to your instances
Email
Customize behavior of inbound and outbound email
Reporting and Analytics
Create visual representations of your data

2. Enter **update** in the search box. The **System Update Sets** menu appears.
3. Click **Retrieved Update Sets**. In the Related Links, Import Update Set from XML link appears.



4. Click Import Update Set from XML.

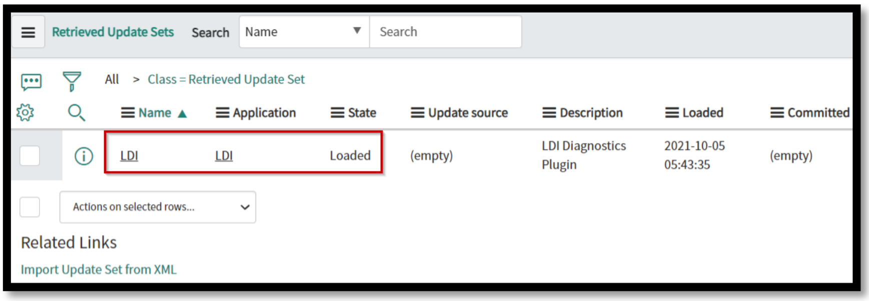


Importing records from an XML file will not run Business Rules

Step 1: Choose file to upload

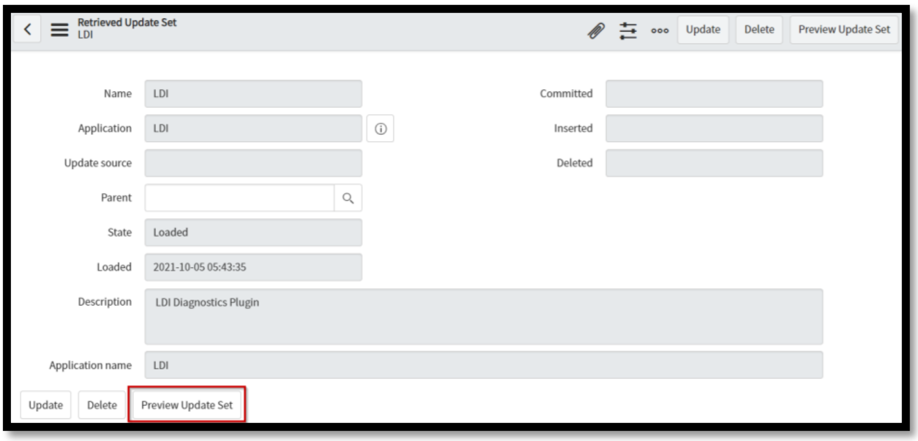
Step 2: Upload the file

5. Click **Choose file**, and then click **Upload.** After the file is imported, the LDI application appears in the list.


Retrieved Update Sets
Search
Name
Search
All
> Class = Retrieved Update Set
Actions on selected rows...
Related Links
Import Update Set from XML

Name ▲	Application	State	Update source	Description	Loaded	Committed
LDI	LDI	Loaded	(empty)	LDI Diagnostics Plugin	2021-10-05 05:43:35	(empty)

6. Click **LDI**. The LDI record appears in the ServiceNow application.



Name: LDI

Application: LDI

Update source:

Parent:

State: Loaded

Loaded: 2021-10-05 05:43:35

Description: LDI Diagnostics Plugin

Application name: LDI

Committed:

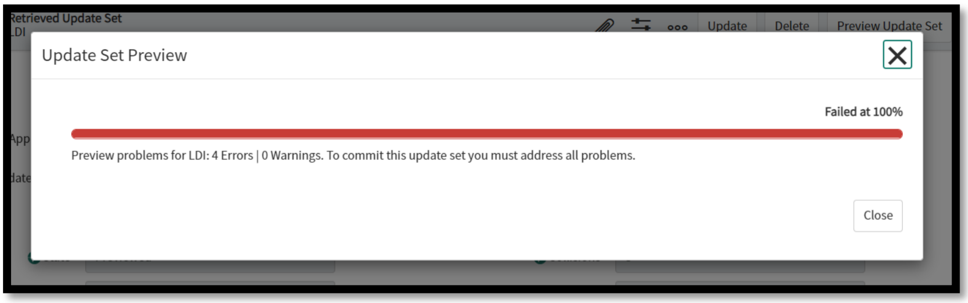
Inserted:

Deleted:

Note: You can update, delete, or get a preview of the LDI update sets.

7. Click Preview Update Set.

Note: The preview fails if there are errors during import of LDI XML file.

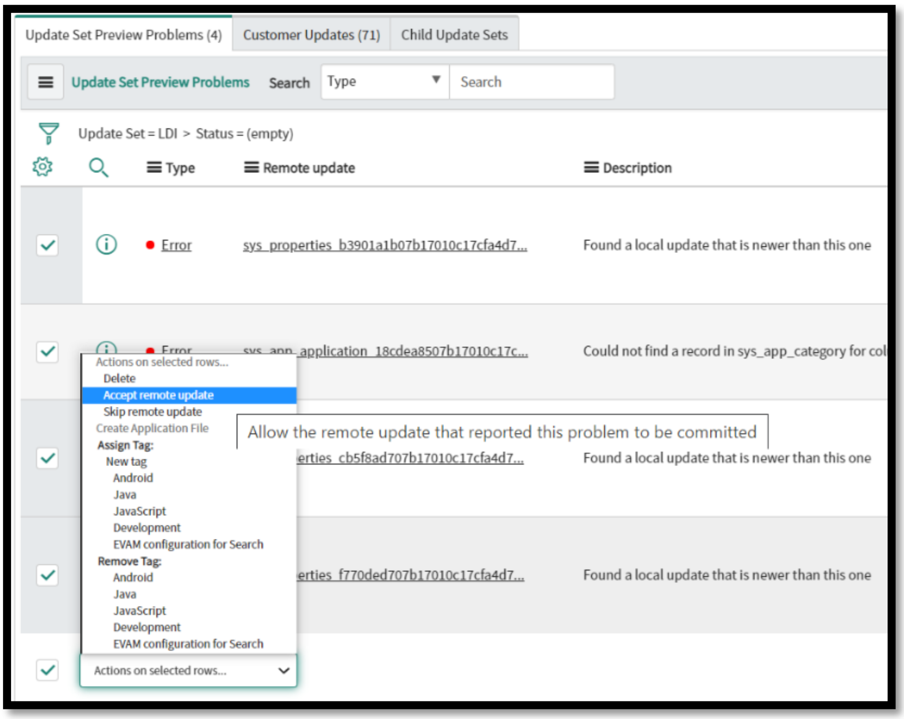


Update Set Preview

Failed at 100%

Preview problems for LDI: 4 Errors | 0 Warnings. To commit this update set you must address all problems.

8. To resolve the errors, select all errors in the tab, click **Update Set Preview Problems.**

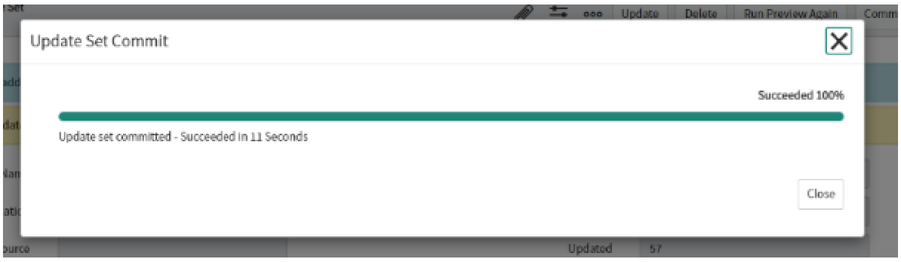


Update Set = LDI > Status = (empty)

Type	Remote update	Description
Error	sys_properties_b3901a1b07b17010c17cfa4d7...	Found a local update that is newer than this one
Error	sys_app_application_18cdea8507b17010c17c...	Could not find a record in sys_app_category for col
	erties_cb5f8ad707b17010c17cfa4d7...	Found a local update that is newer than this one
	erties_f770ded707b17010c17cfa4d7...	Found a local update that is newer than this one

Allow the remote update that reported this problem to be committed

9. Click Accept remote update.



Update Set Commit

Succeeded 100%

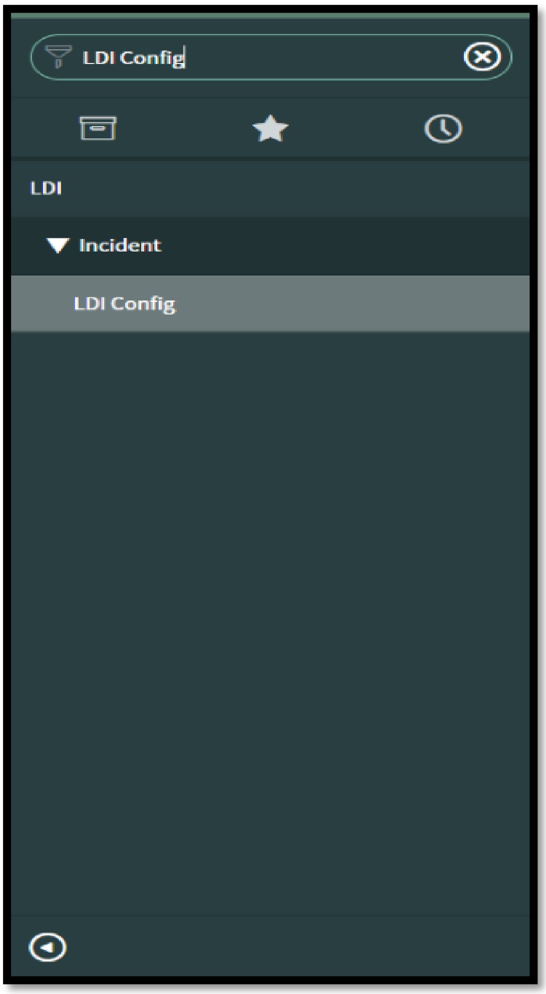
Update set committed - Succeeded in 11 Seconds

10. Click **Commit**. The update set is successfully commited.

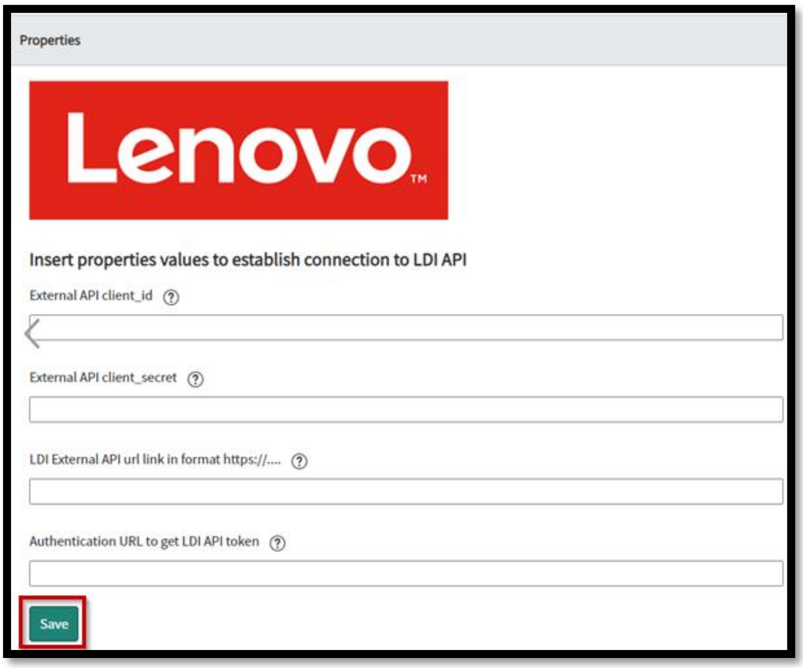
7.16.4 Authenticate LDI API Credentials in ServiceNow

This section explains how to add the LDI API credential in the ServiceNow instance to setup LDI ServiceNow plugin.

1. In the search box, enter **LDI Config**. The **LDI Config** tab appears.



2. Click **LDI Config**. The **Properties** page appears. In this page, enter credentials of LDI API to establish connection between ServiceNow and LDI platform.


Properties

Insert properties values to establish connection to LDI API

External API client_id

External API client_secret

LDI External API url link in format https://....

Authentication URL to get LDI API token

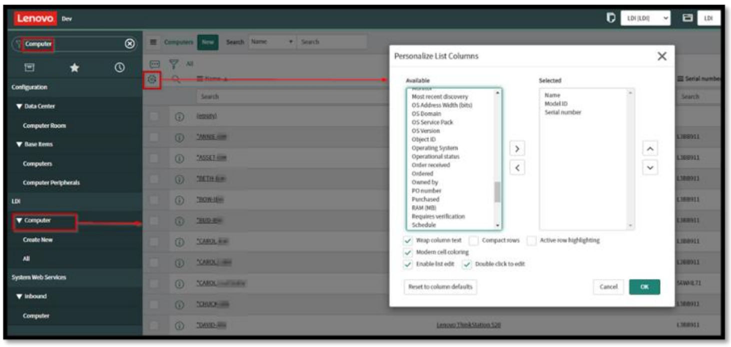
3. Enter LDI API Client ID.

Note: To generate LDI API credetials, refer to Get API Credentials.

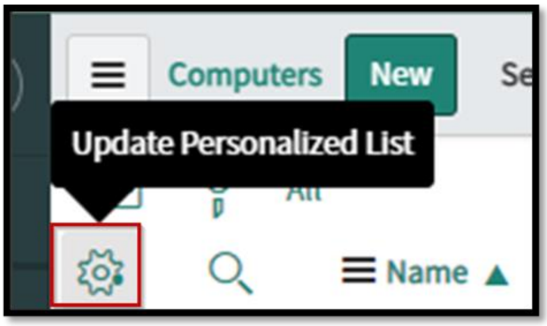
7.16.5 Synchronize Assets in ServiceNow and LDI

Refer Prerequisites section before proceeding ahead.

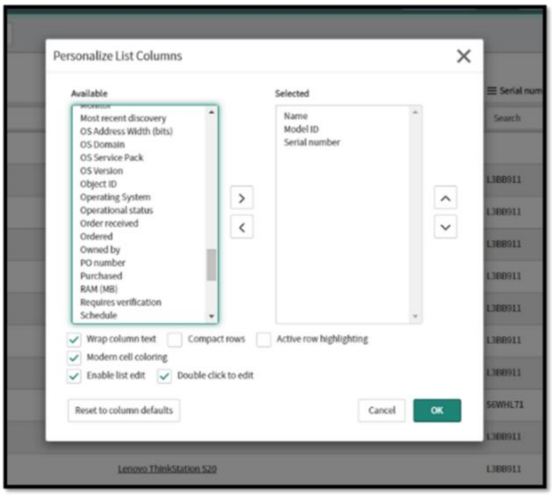
11. Log in to ServiceNow instance.
12. In the search box, enter **computer**. The **Computer** tab appears in the navigation menu.



13. Click **Computer** in the navigation menu. The list of Assets appears in the pane.



14. Click the **Settings** icon. The **Personalize List Columns** window appears.



Personalize List Columns

Available

- Most recent discovery
- OS Address Width (bits)
- OS Domain
- OS Service Pack
- OS Version
- Object ID
- Operating System
- Operational status
- Order received
- Ordered
- Owned by
- PO number
- Purchased
- RAM (MB)
- Requires verification
- Schedule

Selected

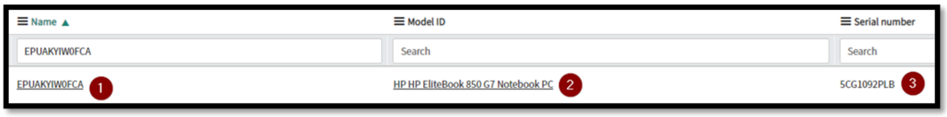
- Name
- Model ID
- Serial number

☑ Wrap column text ☐ Compact rows ☐ Active row highlighting

☑ Modern cell coloring

☑ Enable list edit ☑ Double click to edit

Note: The checkboxes shown in the screenshot are marked by default.



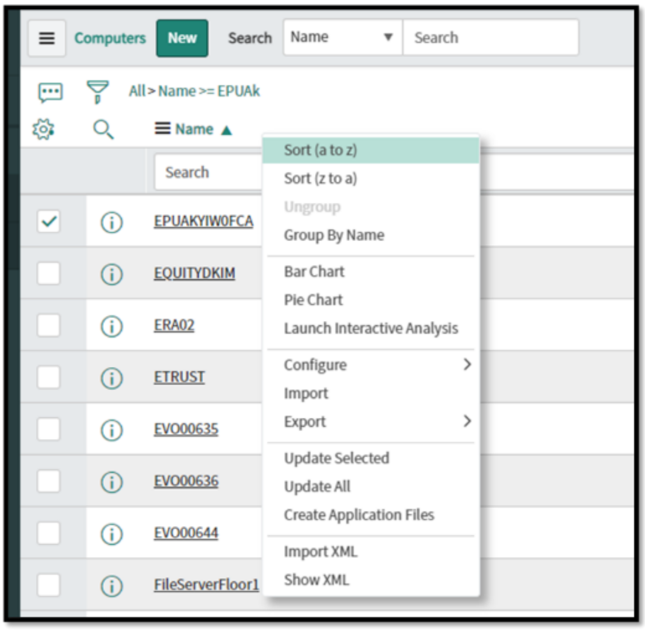
☰ Name ▲	☰ Model ID	☰ Serial number
EPUAKYIW0FCA	Search	Search
EPUAKYIW0FCA 1	HP HP EliteBook 850 G7 Notebook PC 2	5CG1092PLB 3

1. Name of the Asset. For example, EPUAKYIW0FCA
2. Model ID of the Asset – HP EliteBook 850G7 Notebook
3. Serial Number of the Asset – 5CG1092

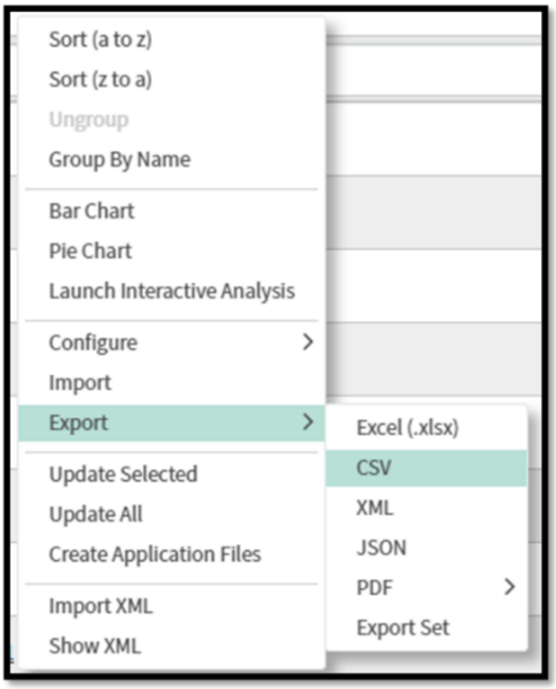
You can search an asset by the Name, Model ID, or Serial Number. Choose assets you want to synchronize by using filters.

Important Note: Do not apply filter if you want to synchronize all.

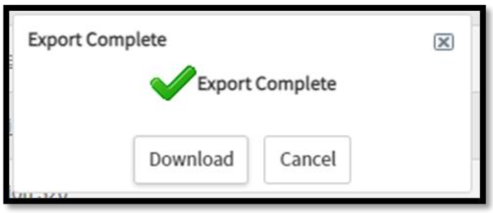
4. Mark the checkboxes to select Assets(s) that you want to synchronize with LDI platform.



5. Right-click the **Export** tab. A side menu appears. In the context menu, choose **Export → CSV**.



6. Select the type of format of the file to be exported. For example, CSV.



7. Click **Download.** The file is downloaded on the device.

The format of the ServiceNow file is:

```
"name","model_id","serial_number"
"EPUAKYIW0FCA","HP HP EliteBook 850 G7 Notebook PC","5CG1092PLB"
```

```
DEVICE NAME, MACHINE TYPE, SERIAL NUMBER, GROUP
EPUAKYIW0FCA, HP EliteBook 850 G7 Notebook PC,5CG1092PLB,
EPBYMINW150E,HP EliteBook 850 G7 Notebook PC,5CG1092PMP,Office1
```

7.16.6 Mandatory Requirements for LDI CSV Format

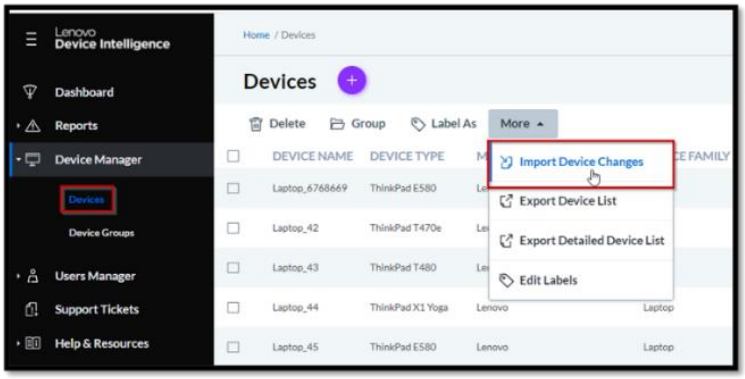
If the name of a device in LDI and ServiceNow is different, then the device name can be changed automatically using the CSV file.

Important Notes:

- Only underscore (_) and dash (-) symbols are allowed.
- To upgrade DEVICE NAME automatically, MACHINE TYPE must be model_id, and SERIAL NUMBER must be equal to serial_number.

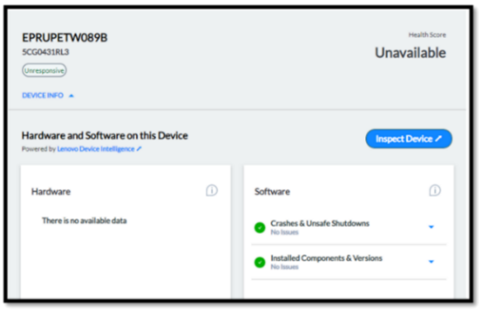
7.16.7 Update Asset Information from ServiceNow to LDI Account

1. Log in to LDI account.
2. Click **Devices** in the navigation menu. The **Devices** pane appears.

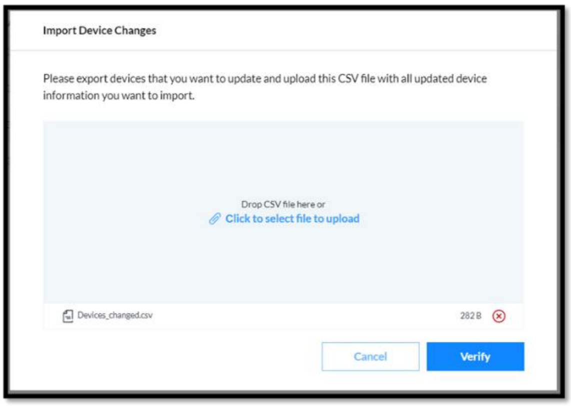


☐	DEVICE NAME	DEVICE TYPE	M	E FAMILY
☐	Laptop_6768669	ThinkPad E580	Le	
☐	Laptop_42	ThinkPad T470e	Le	
☐	Laptop_43	ThinkPad T480	Le	
☐	Laptop_44	ThinkPad X1 Yoga	Lenovo	Laptop
☐	Laptop_45	ThinkPad E580	Lenovo	Laptop

3. Click **More**. The drop-down window appears.
4. Click **Import Device Changes**.

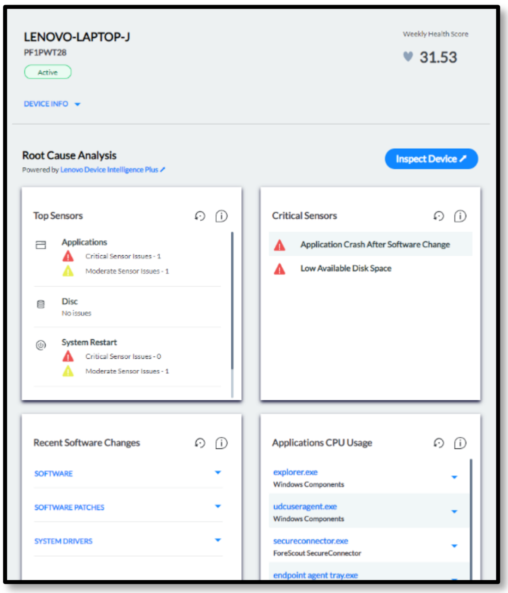

EPRUPETW089B
5CG0431RL3
Unresponsive
DEVICE INFO
Health Score
Unavailable
Hardware and Software on this Device
Powered by Lenovo Device Intelligence
Inspect Device
Hardware
Software
Crashes & Unsafe Shutdowns
No Issues
Installed Components & Versions
No Issues

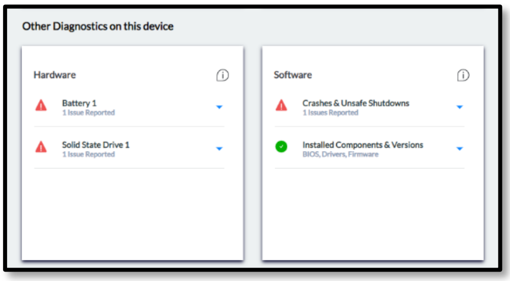
There is no available data



Please export devices that you want to update and upload this CSV file with all updated device information you want to import.

5. Select the file. For example, the CSV file of Assets exported from ServiceNow.
6. Click **Verify**. The file is verified.
7. Click **Yes.** The device information is updated in LDI, and you receive a confirmation email at your registered email ID. ServiceNow receives data of specific device(s) and renders it in the Plugin tab. The LDI ServiceNow plugin is set up.





7.16.8 Integrate ServiceNow into LDI Plus

This feature allows the system to raise a ticket and assign it to the LDI Support team when an incident occurs. It includes tasks such as configuring connection to ServiceNow portal, creating rules that includes sensor management, etc.

Communication between servicenow-integration-service and ServiceNow API occurs using basic authentication. Thus, ServiceNow user credentials are stored in the servicenow-integration-service database and provided each time the API is called.

There is a possibility to use a more secure mechanism - OAuth authentication, when a limited-time token is obtained from OAuth API by credentials and is used in the API calls.

Follow this procedure to support the OAuth authentication:

1. Log in to the ServiceNow portal.
2. Fill-in **Instance URL**.
3. Enter the values for these fields:
    - User ID or Admin Credentials
    - Password
    - Client ID
    - Client Secret

Note:

- The Organization Admin must create a user in ServiceNow for User ID and Password and a client for Client ID and Client Secret.
- The roles must be specified: Admin, Asset, App_service_user, etc. With this set of roles, there is an issue with setting high impact and urgency through the API. When High is requested, Medium is set in the incident.

4. Click **Connect to ServiceNow**. All the filled-in credentials are stores in the database afterward. This way it's possible to receive tokens whenever it's needed.
   Note: This option requires saving user and password, but this user can be controlled at ServiceNow side.

Note: You must have an LDI Admin access privileges to configure and create a rule.

1. Log in to LDI Plus portal.
2. Select **Configuration → Insights & Automations → ServiceNow Incident Rules**. The **SNOW Incident Rules** page appears.
3. Click the **Config Status** drop-down on top-right in the page.
4. Select **Edit Configuration**. The **Configure Connection to ServiceNow** page appears.
5. In the **Add Instance Credentials** section, enter the ServiceNow Instance URL, ServiceNow User ID, and ServiceNow Password.
6. In the **Add Client Credentials** section, enter the ServiceNow Client ID and ServiceNow Client Secret.

   Note: All are mandatory fields.
7. Click **Connect ServiceNow**.

7.16.9 Create a ServiceNow Incident Rule

Note: You need to configure ServiceNow in LDI Plus before creating an incident rule. Refer to Configure ServiceNow Using LDI Plus for more details.

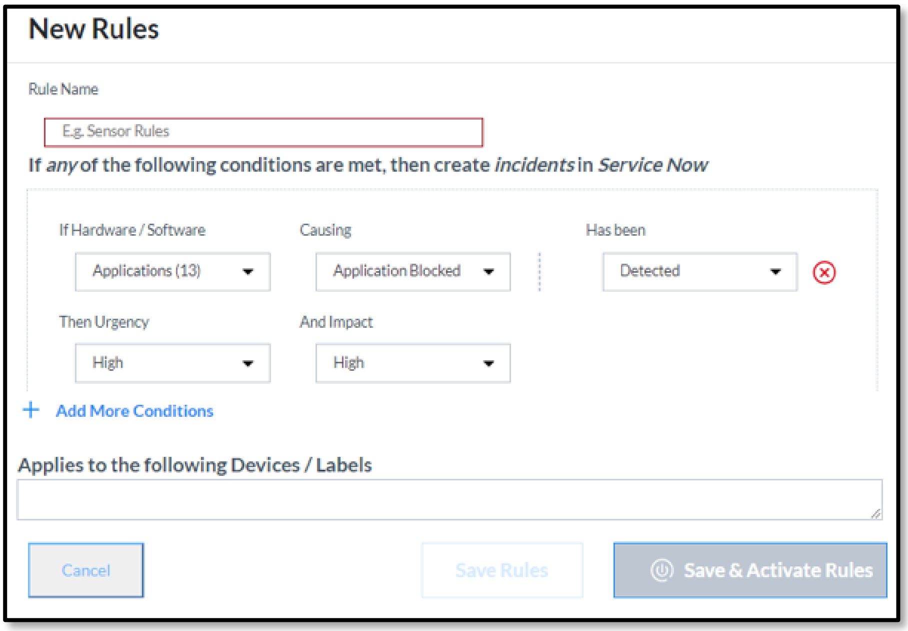
The following table displays the fields in the SNOW Incident Rules page:

Field Name	**Field Description**
Rule Name	The Name of the ServiceNow rule.
Activities Synced	The activities logged by LDI Plus automation. Activities synced displays the number of incidents created when this rule is applied. When the rule is deactivated, this field is not updated.
Actions	• Click the ✎ icon to edit a rule. • Click the ⏻ icon to activate a rule. • Click the ⏻ icon to deactivate a rule. • Click the 🗑 icon to delete a rule.

Note: You can also click the Show Active Rules toggle button on top of the page to display all the active rules for the ServiceNow devices.

To create a rule:

1. In the **SNOW Incident Rules** page, click the + icon. The **New Rules** page appears.
2. Enter the name you want to give to a new rule.
3. Select the conditions from the dropdowns.



New Rules

Rule Name: E.g. Sensor Rules

If *any* of the following conditions are met, then create *incidents* in *Service Now*

If Hardware / Software: Applications (13)

Causing: Application Blocked

Has been: Detected

Then Urgency: High

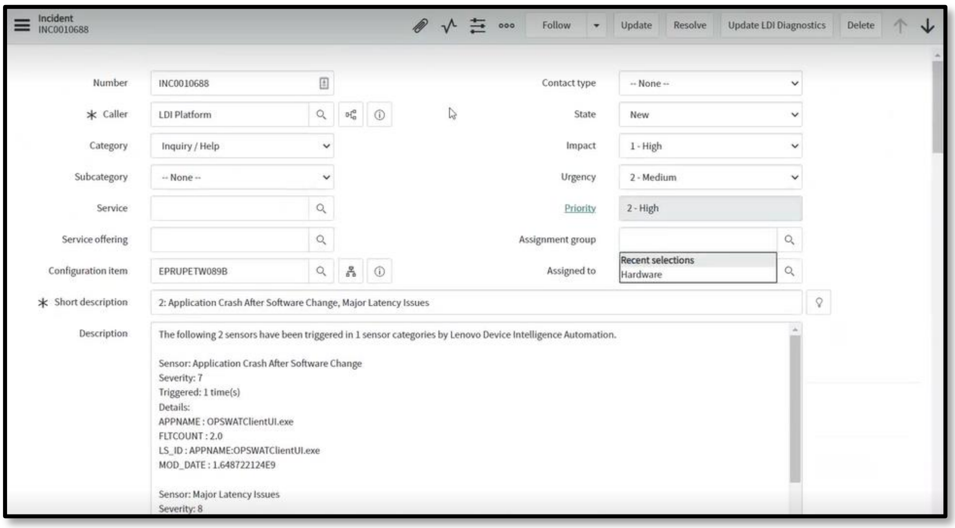
And Impact: High

Applies to the following Devices / Labels

4. Enter the device name or label to which the new rule is applicable.
5. Click **Save Rules**.

7.16.10 Handle an Incident in ServiceNow

The following page displays all the related details of an event created due to occurrence of an incident.



Number	INC0010688	Contact type	-- None --
* Caller	LDI Platform	State	New
Category	Inquiry / Help	Impact	1 - High
Subcategory	-- None --	Urgency	2 - Medium
Service		Priority	2 - High
Service offering		Assignment group	
Configuration item	EPRUPETW089B	Assigned to	Recent selections Hardware
* Short description	2: Application Crash After Software Change, Major Latency Issues		

Description

The following 2 sensors have been triggered in 1 sensor categories by Lenovo Device Intelligence Automation.

Sensor: Application Crash After Software Change
Severity: 7
Triggered: 1 time(s)
Details:
APPNAME : OPSWATClientUI.exe
FLTCOUNT : 2.0
LS_ID : APPNAME:OPSWATClientUI.exe
MOD_DATE : 1.648722124E9

Sensor: Major Latency Issues
Severity: 8

Note: When you create an incident, the details are updated in the **LDI Diagnostics** tab. You can see this tab at the bottom of page. This tab helps you to take an appropriate actions.

8 LDI Test Drive

8.1 Use cases for LDI Plus Features

This chapter assists you in having the BEST user experience as you explore the LDI Plus digital experience monitoring tool. The primary features of the LDI Plus tool are explained in the form of use cases ensuring high performance of fleets and improving the end-user productivity and satisfaction.

To present the features in a logical and intuitive way, this chapter is grouped into three categories:

As an IT Admin, how do I leverage LDI Plus to better understand:

1. **Fleet-level insights and remediations**:

I want better visibility on my overall IT environment and health status of my entire fleet. What are some of the common and major IT issues that are impacting my fleet today and what are the issues Ican avoid in the future by leveraging Lenovo AI-driven predictive analytics?

2. **Device-level insights and remediations**:

I want to deep-dive into the problematic devices to get a comprehensive picture of the IT anomaliesdetected on that device and to resolve those issues easily and at scale.

3. **End User-experience insights and IT efficiency improvements**:

I want to understand how employees' experience and productivity levels are impacted by IT resource constraints. I also want an easier way to figure out how to right-size my hardware and software resources, so my end-users have what they need to do their job effectively.

8.1.1 Fleet-Level Insigths and Remediations

Dashboard

Use Case 1 : How do I tell what's going on with my overall fleet?

Action: Log in to the LDI Plus tool, the Dashboard displays that provides asummary view of your overall environment. Each widget specifies the category of issues by types: BSOD, Applications, Storage, Batteries etc.

Result: You should see data for all the categories within the Dashboard. Each category has a table and graph with a Blueicon ▶ indicating several current or potential issues.

Use Case 2: How do I determine my fleet's overall health score?

Action: View the OVERALL HEALTH SCORE widget to see the overall fleet healthscore as of that day. Then click the blue arrow next to the Health Score to display the score summary for each subcategory contributing to the fleet's overallhealth score.

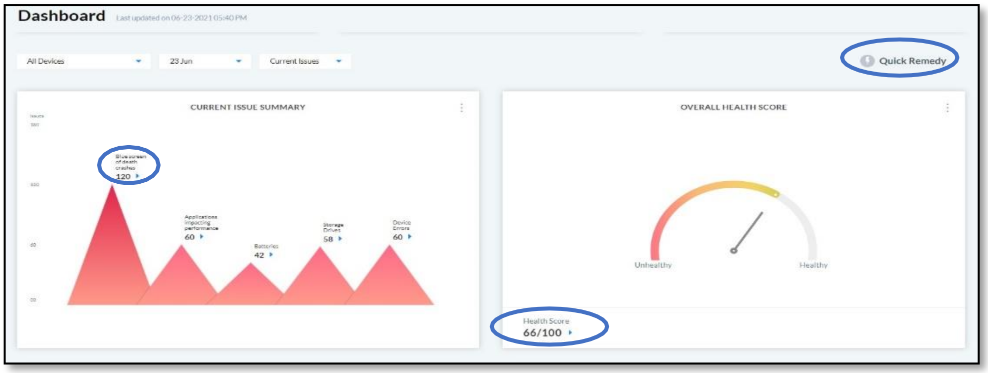
Result: The fleet health summary is calculated by taking an average of the health scores across all active devices for each category. The subcategory breakdown should be helpful to prioritize where to focus to address the Current and Potentialissues in your fleet.

Use Case 3: How do I find out those systems that are most affecting my overall fleet health?

Action: Identify affected systems by clicking on drop down filters in the center of the Dashboard page and filter by Current or Potential Issues. These issues can then be filtered by group, by date and those that have a suggested Quick Remedy ( ) - those issues that have a high-confidence remediation associated with it.

Result: A filtered version of your set criteria will then be displayed on the Dashboard page.

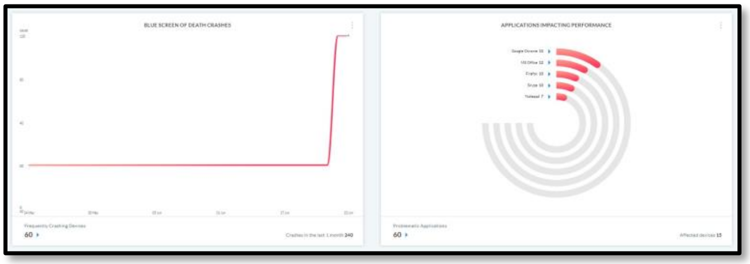
Note: Only the Quick Remedy feature is available when you filter by Potential Issues.

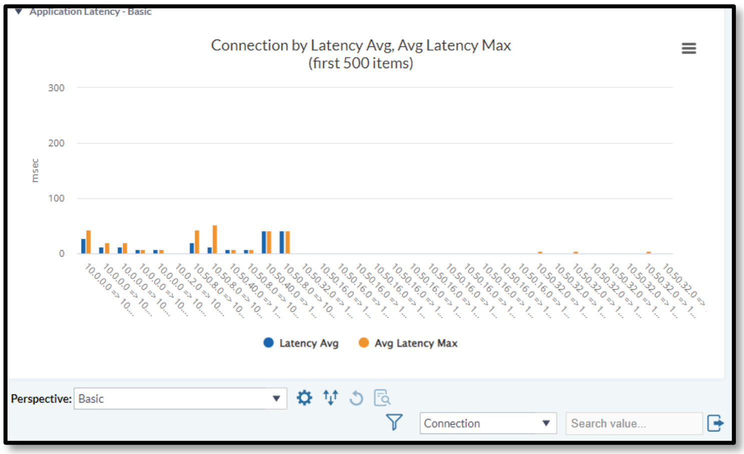


Use Case 4: Where can I see the application latency details for devices?

Action: Select User Experience → Device Overview → Application Latency

Result: The page displays the latency details for the devices based on the set criteria.


BLUE SCREEN OF DEATH CRASHES
Frequently Crashing Devices
60
Crashes in the last 1 month 240
APPLICATIONS IMPACTING PERFORMANCE
Google Chrome 15
MS Office 12
Firefox 10
Skype 10
Notepad 7
Problematic Applications
60
Affected devices 15



Perspective: Basic

Use Case 5: How can I get the details of the devices that are remotely logged in?

Action: Select Dashboard → Remote Work

Result: The Remote Work page displays the following details:

They are:

DEM (User Experience Trend) – A representation in the form of bar graph that indicates the user experience of using a device or group of devices based on the number of days of data gathered from the device or fleet of devices. As you discover issues and fix them the trend will change over the time.

Top 5 Health Impacts – A pie-chart representation of top 5 impacts to the end-user experience. A bigger slice of pie chart indicates that greater attention must be paid to that metric as it is negatively impacting user experience more than others.

Digital Experience Tools – A pie-chart presentation of the important metrics or parameters that impact remote work/collaboration, like office connectivity, security and compliance, productivity and collaboration and device. The metrics that have larger share of the pie-chart are impacting more, because more problems are occurring there.

Machine Sizing – A pie-chart presentation machine sizing for the system or group of devices in context to the hardware utilized. Whether it is over provisioned, under provisioned or is right-sized.

Use Case 6: Does LDI Plus help in taking proactive approaches?

Action: Select Dashboard → Proactive Support

Result: The **Proactive Support** page displays the following details:

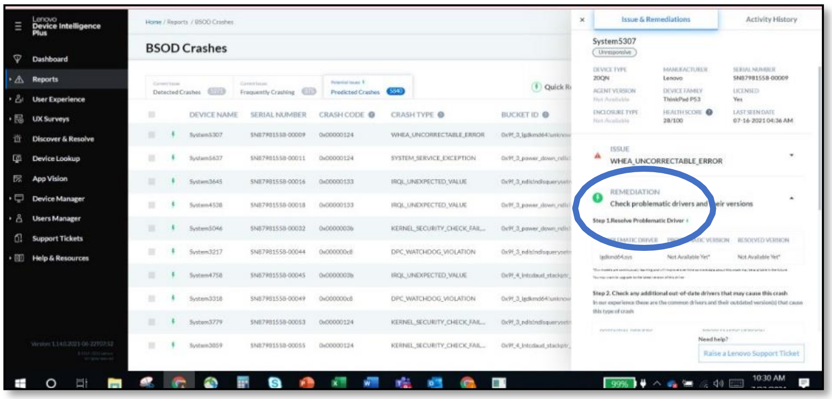
- Percentage of devices not on the latest app version
- Number of devices over provisioned, under provisioned and right sized
- Percentage of systems patched and unpatched

- Average daily active hours and average daily impacted hours

These details enable you to take proactive actions to remediate your device issues.

Issues & Reports

In each widget displayed on the dashboard, clicking on the blue arrows within the table pulls up the corresponding report that lists the affected devices in that category along with details about the specific issue and in some cases, other filter tabs are also available. Another navigation path to display specific reports is to simply click Reports in the navigation pane on the left side of the screen. You can also select an individual system to reveal the issue tray and further details about the device issues as well as suggested remediations for those issues.



BSOD Crashes

DEVICE NAME	SERIAL NUMBER	CRASH CODE	CRASH TYPE	BUCKET ID
System5307	SN87981558-00009	0x00000124	WHEA_UNCORRECTABLE_ERROR	0x9f_3_igdkmd64!unknow
System5637	SN87981558-00011	0x00000124	SYSTEM_SERVICE_EXCEPTION	0x9f_3_power_down_ndis!
System3645	SN87981558-00016	0x00000133	IRQL_UNEXPECTED_VALUE	0x9f_3_ndis!ndisqueryset
System4538	SN87981558-00018	0x00000133	IRQL_UNEXPECTED_VALUE	0x9f_3_power_down_ndis!
System5046	SN87981558-00032	0x0000003b	KERNEL_SECURITY_CHECK_FAIL...	0x9f_3_power_down_ndis!
System3217	SN87981558-00044	0x000000c8	DPC_WATCHDOG_VIOLATION	0x9f_3_ndis!ndisqueryset
System4758	SN87981558-00045	0x0000003b	IRQL_UNEXPECTED_VALUE	0x9f_4_intcdaud_stackptr_
System3318	SN87981558-00049	0x000000c8	DPC_WATCHDOG_VIOLATION	0x9f_3_igdkmd64!unknow
System3779	SN87981558-00053	0x00000124	KERNEL_SECURITY_CHECK_FAIL...	0x9f_3_ndis!ndisqueryset
System3059	SN87981558-00055	0x00000124	KERNEL_SECURITY_CHECK_FAIL...	0x9f_4_intcdaud_stackptr_

System5307
Unresponsive

DEVICE TYPE	MANUFACTURER	SERIAL NUMBER
20QN	Lenovo	SN87981558-00009
AGENT VERSION	DEVICE FAMILY	LICENSED
Not Available	ThinkPad P53	Yes
ENCLOSURE TYPE	HEALTH SCORE	LAST SEEN DATE
Not Available	28/100	07-16-2021 04:36 AM

ISSUE
WHEA_UNCORRECTABLE_ERROR

REMEDIATION
Check problematic drivers and their versions

Step 1.Resolve Problematic Driver

PROBLEMATIC DRIVER	PROBLEMATIC VERSION	RESOLVED VERSION
igdkmd64.sys	Not Available Yet*	Not Available Yet*

Step 2. Check any additional out-of-date drivers that may cause this crash
In our experience these are the common drivers and their outdated version(s) that cause this type of crash

Issue-type reports for all systems with current or potential issues that are tracked within the Dashboard (i.e. BSOD, Applications, Batteries, Storage & Device Errors) can also be filtered and exported.

BSOD Crashes

DEVICE NAME	SERIAL NUMBER	CRASH CODE	CRASH TYPE	BUCKET ID	DEVICE GROUP	CRASHED ON

Discover and Resolve – The Sea of Sensors

Use Case 4: What devices within my fleet are showing issues, why, and what can Ido to fix them?

Action: Click **Discover and Resolve** in the navigation pane.

Results: The Discover and Resolve Overview pane appears. All currently *activated and triggered* sensor categories are displayed in the top in the **Sensor Overview** section of the pane. Click on the arrow next to the sensor section to expand that section and expose the specific sensors activated. You can see all devices impacted by each triggered sensor within the fleet. To see a list of ALL sensors being monitored in the fleet, uncheck the box at the top that says, Show Activated Sensors Only.

Use Case 5: Which sensors are being triggered most common?

Action: Below the Sensor Overview section in the Top Sensors and Systems section, is the Most Common Sensers section. Here you see a list of the most triggered sensors in the fleet and the count of how many systems impacted. Double-clicking on any of the sensors takes you to the Sensor Details submenu in the left navigation pane and you can read a description of what the sensor is monitoring and, in many cases, a suggested fix.

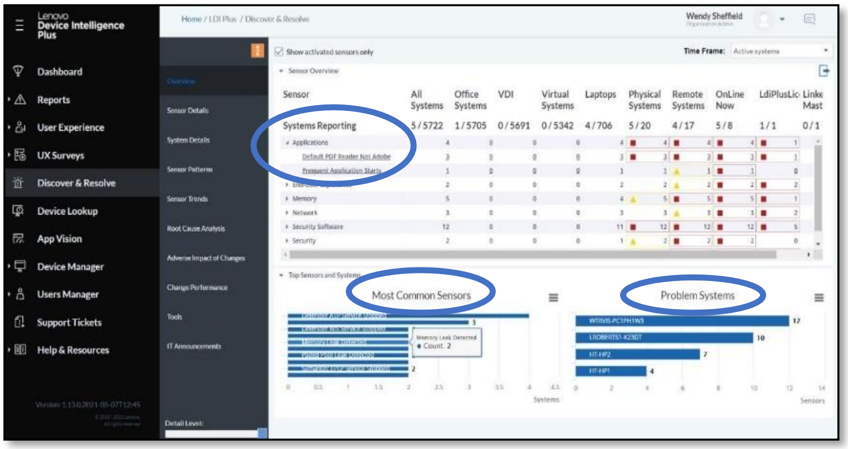
Use Case 6: Which PCs are giving me the most problematic issues?

Action: In the **Problem Systems** section, you see a list of the devices in your fleet with the most sensors active in the associated time frame with a count of how many sensors are active on each device.

Use Case 7: What can I do to keep a sensor issue from triggering on a device again?

Action: Double-click on the individual sensor that you want to explore under the Sensor Overview section or the Most Common Sensors section of the pane.

Results: The Sensors Detail page appears, which shows a list of the affected devices and a description of the sensor with remediation steps listed in the description. You can also view the location of the devices and the trend over time of how often this sensor was triggered on them.



☑ Show activated sensors only

Time Frame: Active systems

Sensor Overview

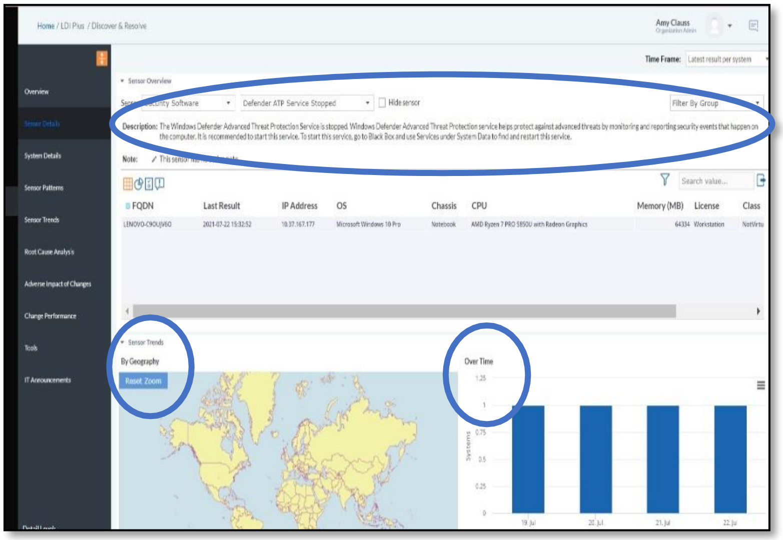
Sensor	All Systems	Office Systems	VDI	Virtual Systems	Laptops	Physical Systems	Remote Systems	OnLine Now	LdiPlusLic	Linke Mast
Systems Reporting	5 / 5722	1 / 5705	0 / 5691	0 / 5342	4 / 706	5 / 20	4 / 17	5 / 8	1 / 1	0 / 1
Applications	4	0	0	0	4 ■	4 ■	4 ■	4 ■	1	
Default PDF Reader Not Adobe	3	0	0	0	3 ■	3 ■	3 ■	3 ■	1	
Frequent Application Starts	1	0	0	0	1	1 ▲	1 ■	1	0	
End-User Experience	2	0	0	0	2	2 ▲	2 ■	2 ■	2	
Memory	5	0	0	0	4 ▲	5 ■	5 ■	5 ■	1	
Network	3	0	0	0	3	3 ▲	3 ■	3 ■	2	
Security Software	12	0	0	0	11 ■	12 ■	12 ■	12 ■	5	
Security	2	0	0	0	1 ▲	2 ■	2 ■	2	0	

8.1.2 Device-level Insights and Remediations

Device Lookup

Use Case 8: I need to help my end-user John Smith determine why his device isrunning so slow today. It was working fine yesterday.

Action: Click **Device Lookup**. Enter the first few characters of the name of the device you want to explore in the **Find System** text box. In this instance, enter Lenovo. Select the device from the list of devices displayed.



Description: The Windows Defender Advanced Threat Protection Service is stopped. Windows Defender Advanced Threat Protection service helps protect against advanced threats by monitoring and reporting security events that happen on the computer. It is recommended to start this service. To start this service, go to Black Box and use Services under System Data to find and restart this service.

FQDN	Last Result	IP Address	OS	Chassis	CPU	Memory (MB)	License	Class
LENOVO-C9OUJV6O	2021-07-22 15:32:52	10.37.167.177	Microsoft Windows 10 Pro	Notebook	AMD Ryzen 7 PRO 5850U with Radeon Graphics	64334	Workstation	NotVirtu

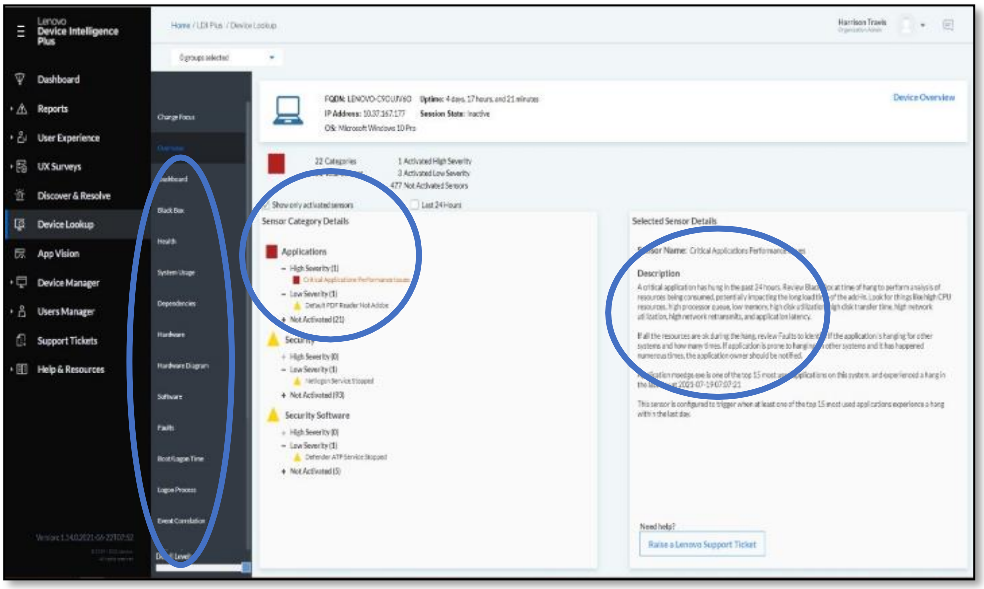
Results: This connects you directly to the system selected where detailed information is shown in the Overview sub menu within the Device Lookup main menu.

You see a list of activated sensors for the individual device that was selected and a description of that sensor on the right side. Click and explore other aspects of the focus device listed in the sub navigation tree for Device Lookup.

For example:

Health submenu - see the amount of Quality Time (ie: end-user productivity time) impacted by the issues picked up by the sensors

Black box submenu – go back in time to see when sensors were triggered to then correlate any actions executed prior to that which may have caused it (eg: new bios upgrade)



FQDN: LENOVO-C9OUJV6O **Uptime:** 4 days, 17 hours, and 21 minutes
IP Address: 10.37.167.177 **Session State:** Inactive
OS: Microsoft Windows 10 Pro

22 Categories
1 Activated High Severity
3 Activated Low Severity
477 Not Activated Sensors

☑ Show only activated sensors ☐ Last 24 Hours

Sensor Category Details

- Applications
  - High Severity (1)
    - Critical Application Performance Issues
  - Low Severity (1)
    - Default PDF Reader Not Adobe
  - Not Activated (21)
- Security
  - High Severity (0)
  - Low Severity (1)
    - Netlogon Service Stopped
  - Not Activated (93)
- Security Software
  - High Severity (0)
  - Low Severity (1)
    - Defender ATP Service Stopped
  - Not Activated (5)

Selected Sensor Details

Sensor Name: Critical Applications Performance Issues

Description

A critical application has hung in the past 24 hours. Review Black box at time of hang to perform analysis of resources being consumed, potentially impacting the long load time of the add-in. Look for things like high CPU resources, high processor queue, low memory, high disk utilization, high disk transfer time, high network utilization, high network retransmits, and application latency.

If all the resources are ok during the hang, review Faults to identify if the application is hanging for other systems and how many times. If application is prone to hanging on other systems and it has happened numerous times, the application owner should be notified.

Application msedge.exe is one of the top 15 most used applications on this system, and experienced a hang in the last day at 2021-07-19 07:07:21

This sensor is configured to trigger when at least one of the top 15 most used applications experience a hang within the last day.

8.1.3 User Experience Insights and Improvements

Fleet-view Dashboard

Use Case 9: How do I measure how all the performance issues occurring across the fleet are impacting my end-user’s experience (ie: ability to be productive without IT system constraints) and what are the biggest issue areas impacting their experience?

Action: Select **User Experience → FleetView**, you see the following details:

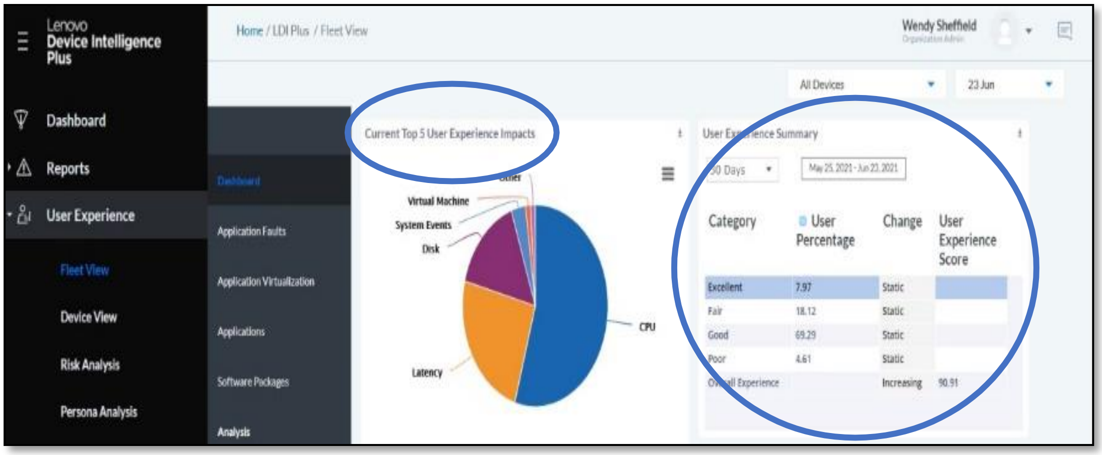
- User Experience Summary Score
- Top 5 User Experience Impacts
- Several ‘Trending’ analytics widgets

Results

User Experience Summary Score - reveals a breakdown of what the overall end-user User Experience Score is, what percentage of users fall into each category, and whether the trend is increasing or decreasing. A rating of Excellent means that less than 10% of the end-user’s time in aggregate across the fleet is being impacted by resource constraint (Fair = 15%,Good = 20%, Poor = >20%).

Top 5 User Experience Impacts – helps IT teams prioritize the top areas they should focus on that are impacting the User Experience scores the most. (i.e. CPU, Latency, Disk error etc.) Hovering over the pie chart reveals the average amount of hours impacted in a typical workweek.

Trending Analytics widgets – peruse the page and you can see other trendinganalyses impacting end-user’s experiences with the ability to click and drilldown for further details.



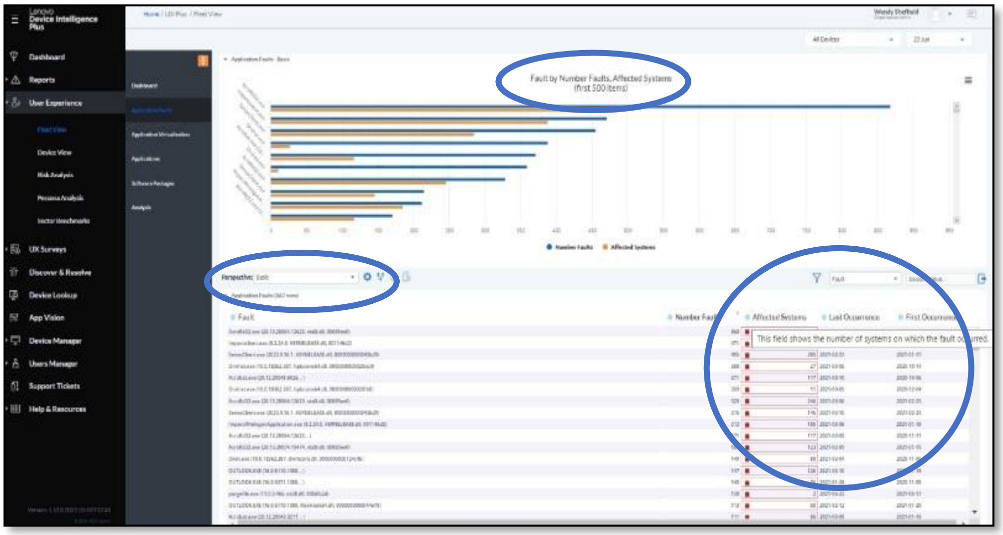
Category	User Percentage	Change	User Experience Score
Excellent	7.97	Static	
Fair	18.12	Static	
Good	69.29	Static	
Poor	4.61	Static	
Overall Experience		Increasing	90.91

Use Case 10: What are the top applications causing issues within myenvironment?

Action: Within User Experience > Fleet View, select Application Faults

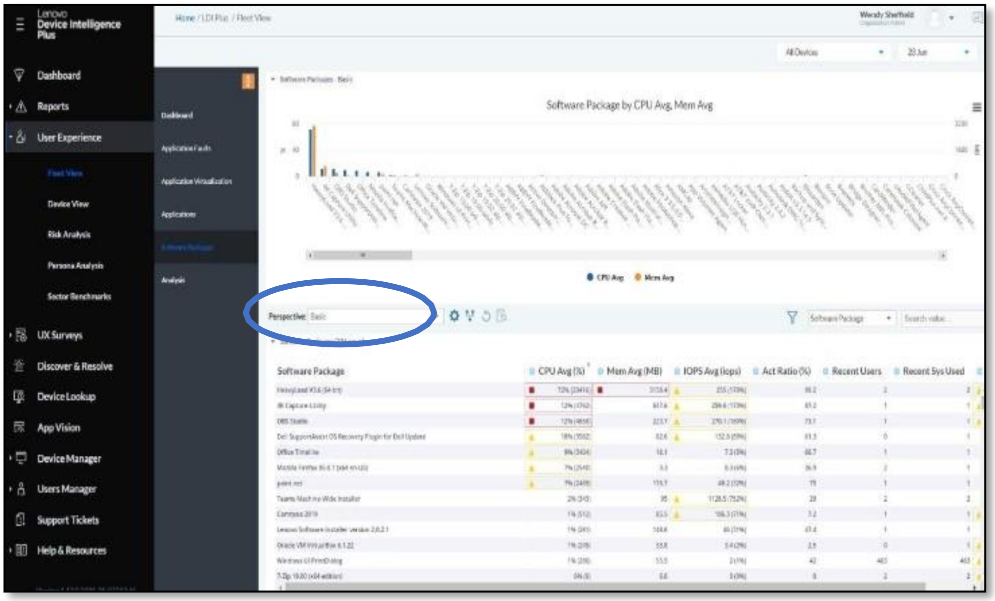
Results: View the list of applications causing faults to occur, the number of faultsthey are causing on which systems, and the first and last time the fault occurred. Clicking on any line item will show you all the system IDs the fault is occurring on.

Filter different data points by clicking on the Perspective dropdown menu. Remember you can also double-click next to any detail with a blue dot next to itfor further drilldown.



Use Case 11: Which of my Software applications are consuming most of my systems resources?

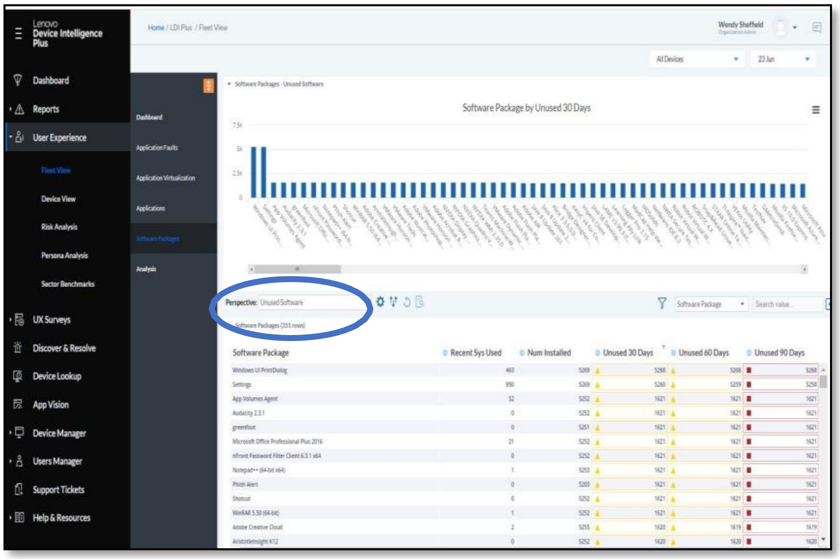
Action: Within User Experience -> Fleet View click on **Software Packages.**



Use Case 12: What software applications are being underutilized by my end-users? Perhaps this is an area to right-size my investment and save money.

Action: Look at different Perspectives – From the Perspective drop-down, select Unused Software

Result: Screen displays the number of devices that have installed a particularsoftware package vs the number of devices using that software package(or not). It will also show if the software has been unused for the last 30/60/90 days. Removing licenses for unused software packages could potentially bring a cost saving to your organization.



Perspective: Unused Software

Software Packages (351 rows)

Software Package	Recent Sys Used	Num Installed	Unused 30 Days	Unused 60 Days	Unused 90 Days
Windows UI PrintDialog	463	5269	5268	5268	5268
Settings	950	5269	5260	5259	5258
App Volumes Agent	52	5252	1621	1621	1621
Audacity 2.3.1	0	5252	1621	1621	1621
greenfoot	0	5251	1621	1621	1621
Microsoft Office Professional Plus 2016	21	5252	1621	1621	1621
nFront Password Filter Client 6.3.1 x64	0	5252	1621	1621	1621
Notepad++ (64-bit x64)	1	5253	1621	1621	1621
Phish Alert	0	5203	1621	1621	1621
Shotcut	0	5252	1621	1621	1621
WinRAR 5.50 (64-bit)	1	5252	1621	1621	1621
Adobe Creative Cloud	2	5255	1620	1619	1619
AristotleInsight K12	0	5252	1620	1620	1620

Persona Analysis, Hardware, and Software Rightsizing

Use Case 13: How do I figure out whether we've provisioned the right configuration of software and hardware resources for my end-users to do their job effectively? First understand how your end-users are segmented by role and workstyle. Then, you can view common usage patterns among them to see what IT resources they are mostly using and whether they are constantly reaching recommended thresholds or not. If yes, then you know you should probably make some adjustments to what you have provisioned that user group.

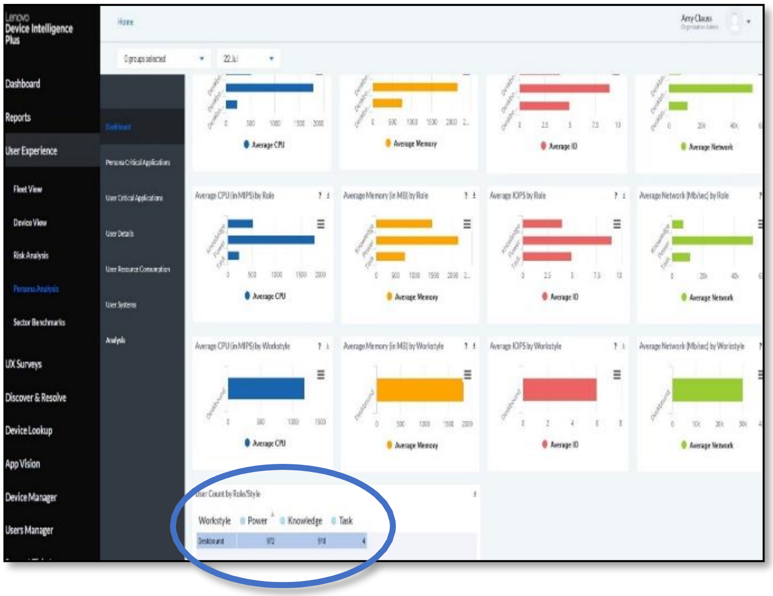
Action: In **User Experience,** click Persona Analysis. The Dashboard appears.

Result: View User Count by Role or Style in the bottom of the pane. Here, you see a count of users segmented by deskbound vs non-deskbound – those likely having a laptop or not. Users are also segmented into Power, Knowledge or Task Workers roles, or personas. The graphs also show the average usage of a specific IT resource by each of these user segments.

The user segmentation is based on the observed behaviours and consumption pattern of certain IT resources which LDI Plus is constantly monitoring. Power users are those that tax their system heavily and meet higher thresholds for CPU, Memory, and I/O consumption. Task workers are those that use less than 10 applications on their system and have much lower consumption rates. KnowledgeWorkers are all those that fall in between Power and Task workers.

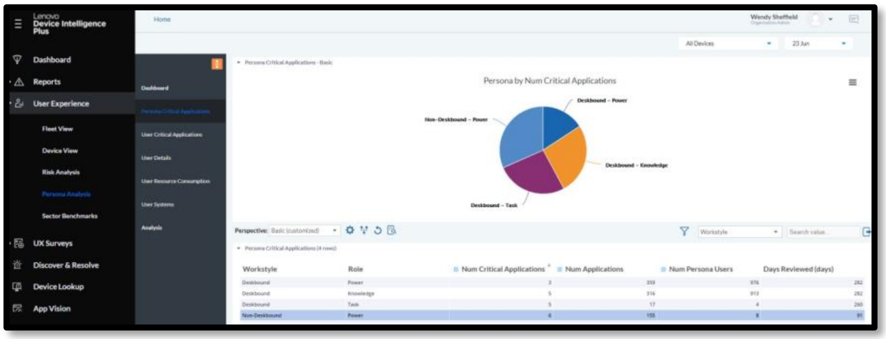
Action: Now that you understand how your end-users will be segmented, under the User Experience section in the navigation tree**, c**lick **Persona Analysis** then click **Persona Critical Applications**. This helps you better the usage patterns of the **applications** you provide to your end-users in their Persona segments.

Result: The Persona Critical Apps Window reveals the number of both overall and critical applications each Workstyle Role uses, how many of each persona type uses them and on average how many days or year they use them. If you choose any workstyle and double-click, you see a new window open which also tell you how much focus time in hours or week each persona spends in that application.


Lenovo Device Intelligence Plus
Home
Amy Claus
0 groups selected
22 Jul
Dashboard
Reports
User Experience
Fleet View
Device View
Risk Analysis
Persona Analysis
Sector Benchmarks
UX Surveys
Discover & Resolve
Device Lookup
App Vision
Device Manager
Users Manager
Dashboard
Persona Critical Applications
User Critical Applications
User Details
User Resource Consumption
User Systems
Analysis
Average CPU
Average Memory
Average IO
Average Network
Average CPU (in MIPS) by Role
Average Memory (in MB) by Role
Average IOPS by Role
Average Network (Mb/sec) by Role
Average CPU (in MIPS) by Workstyle
Average Memory (in MB) by Workstyle
Average IOPS by Workstyle
Average Network (Mb/sec) by Workstyle

User Count by Role/Style

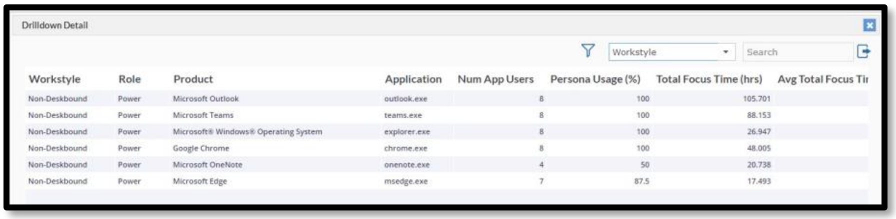
Workstyle	Power	Knowledge	Task
Deskbound	972	918	4



Perspective: Basic (customized)

Persona Critical Applications (4 rows)

Workstyle	Role	Num Critical Applications	Num Applications	Num Persona Users	Days Reviewed (days)
Deskbound	Power	3	359	976	282
Deskbound	Knowledge	5	316	913	282
Deskbound	Task	5	17	4	280
Non-Deskbound	Power	6	155	8	81



Drilldown Detail

Workstyle

Workstyle	Role	Product	Application	Num App Users	Persona Usage (%)	Total Focus Time (hrs)	Avg Total Focus Tir
Non-Deskbound	Power	Microsoft Outlook	outlook.exe	8	100	105.701	
Non-Deskbound	Power	Microsoft Teams	teams.exe	8	100	88.153	
Non-Deskbound	Power	Microsoft® Windows® Operating System	explorer.exe	8	100	26.947	
Non-Deskbound	Power	Google Chrome	chrome.exe	8	100	48.005	
Non-Deskbound	Power	Microsoft OneNote	onenote.exe	4	50	20.738	
Non-Deskbound	Power	Microsoft Edge	msedge.exe	7	87.5	17.493	

Use Case 14: How do I know if I need to do any hardware rightsizing for a specific persona end-user segment?

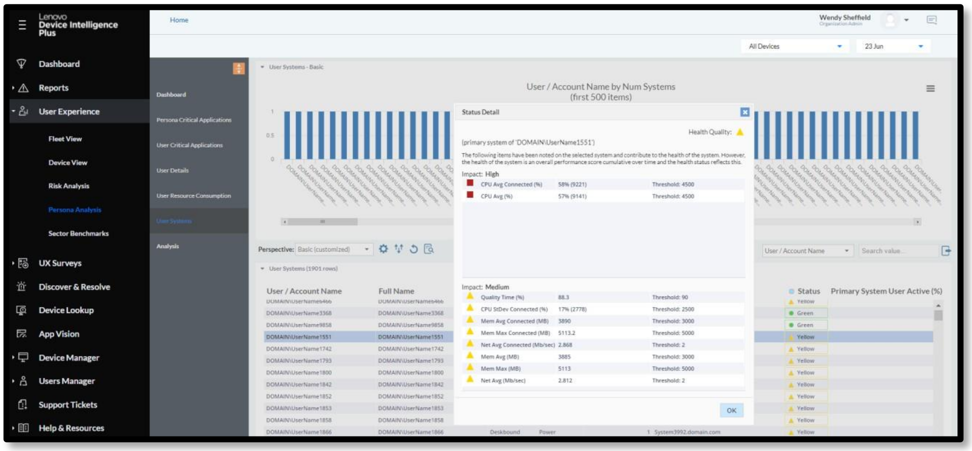
Action: Under the User Experience section in the navigation tree**,** Click on PersonaAnalysis and click on User Systems.

Result: Clicking on the User Systems reveals by Role and Workstyle all the systems and their respective health status with a red, yellow, or green dot. You can then click any system to drill down and see the specific IT resource usage   percentages and thresholds, divided by high or medium impact. This is useful for IT admins to see at-a-glance whether a user is consistently exceeding recommended usage thresholds for any IT resource and then can adjust accordingly with a new device (eg: one with higher CPU processing speed) or component changes within the current device (eg: more memory).

AppVision

Use Case 15: How do I go much deeper into applications to see the most usedones and the system resource consumption required?

Action: Click App Vision in the left-hand navigation tree. The Dashboard reveals the following:



Status Detail

Health Quality: ⚠

(primary system of 'DOMAIN\UserName1551')

The following items have been noted on the selected system and contribute to the health of the system. However, the health of the system is an overall performance score cumulative over time and the health status reflects this.

Impact: **High**

🟥	CPU Avg Connected (%)	58% (9221)	Threshold: 4500
🟥	CPU Avg (%)	57% (9141)	Threshold: 4500

Impact: **Medium**

⚠	Quality Time (%)	88.3	Threshold: 90
⚠	CPU StDev Connected (%)	17% (2778)	Threshold: 2500
⚠	Mem Avg Connected (MB)	3890	Threshold: 3000
⚠	Mem Max Connected (MB)	5113.2	Threshold: 5000
⚠	Net Avg Connected (Mb/sec)	2.868	Threshold: 2
⚠	Mem Avg (MB)	3885	Threshold: 3000
⚠	Mem Max (MB)	5113	Threshold: 5000
⚠	Net Avg (Mb/sec)	2.812	Threshold: 2

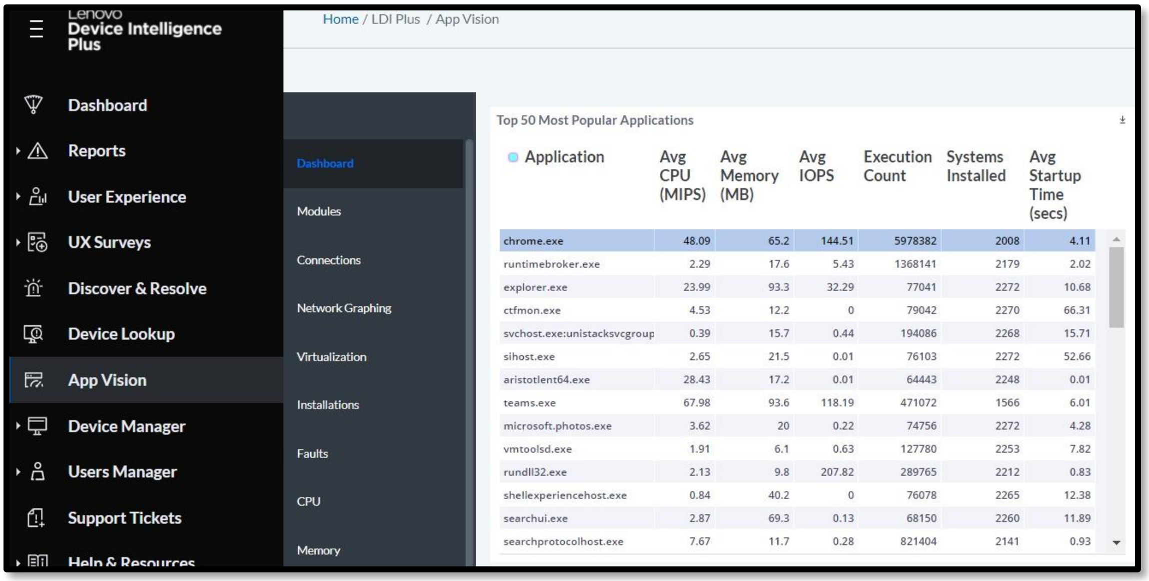
OK

User / Account Name	Full Name					Status	Primary System User Active (%)
DOMAIN\UserName6466	DOMAIN\UserName6466					⚠ Yellow	
DOMAIN\UserName3368	DOMAIN\UserName3368					● Green	
DOMAIN\UserName9858	DOMAIN\UserName9858					● Green	
DOMAIN\UserName1551	DOMAIN\UserName1551					⚠ Yellow	
DOMAIN\UserName1742	DOMAIN\UserName1742					⚠ Yellow	
DOMAIN\UserName1793	DOMAIN\UserName1793					⚠ Yellow	
DOMAIN\UserName1800	DOMAIN\UserName1800					⚠ Yellow	
DOMAIN\UserName1842	DOMAIN\UserName1842					⚠ Yellow	
DOMAIN\UserName1852	DOMAIN\UserName1852					⚠ Yellow	
DOMAIN\UserName1853	DOMAIN\UserName1853					⚠ Yellow	
DOMAIN\UserName1858	DOMAIN\UserName1858					⚠ Yellow	
DOMAIN\UserName1866	DOMAIN\UserName1866	Deskbound	Power	1	System3992.domain.com	⚠ Yellow	

Top 50 most popular Applications by fault count vs. Systems installed

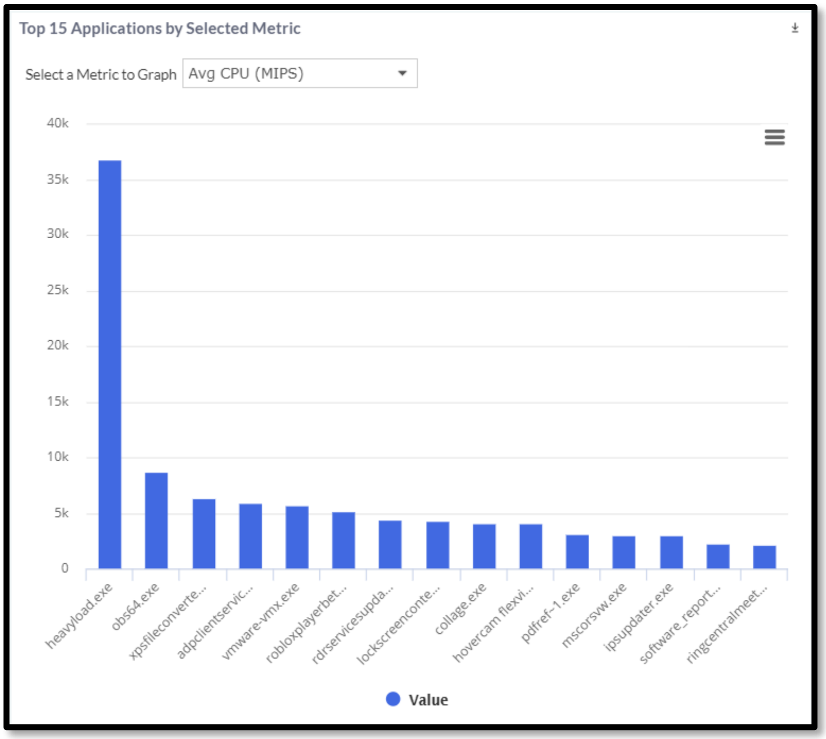
Top 15 application by selected Metric such as average CPU, average. Memory, average IOPS, average start up time, and execution count

Top 50 most popular Applications by fault count vs. Systems installed.



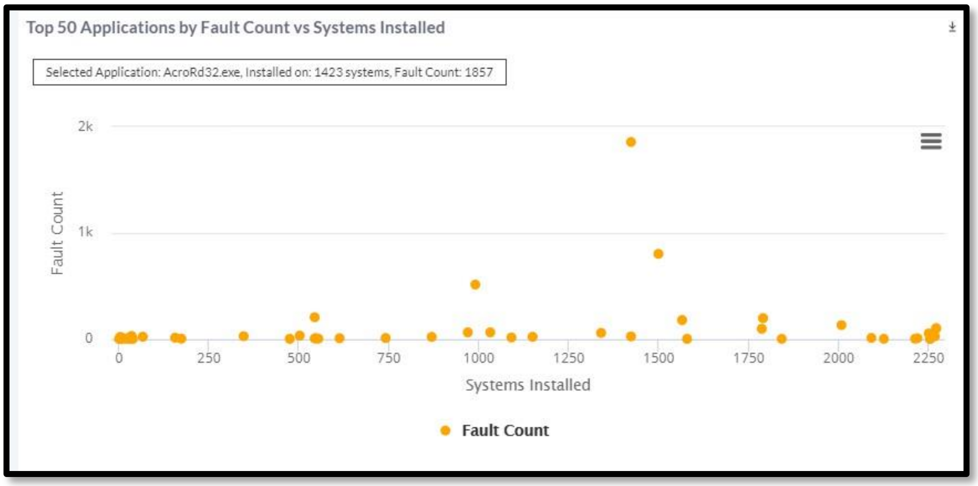
Top 50 Most Popular Applications

Application	Avg CPU (MIPS)	Avg Memory (MB)	Avg IOPS	Execution Count	Systems Installed	Avg Startup Time (secs)
chrome.exe	48.09	65.2	144.51	5978382	2008	4.11
runtimebroker.exe	2.29	17.6	5.43	1368141	2179	2.02
explorer.exe	23.99	93.3	32.29	77041	2272	10.68
ctfmon.exe	4.53	12.2	0	79042	2270	66.31
svchost.exe:unistacksvcgroup	0.39	15.7	0.44	194086	2268	15.71
sihost.exe	2.65	21.5	0.01	76103	2272	52.66
aristotlent64.exe	28.43	17.2	0.01	64443	2248	0.01
teams.exe	67.98	93.6	118.19	471072	1566	6.01
microsoft.photos.exe	3.62	20	0.22	74756	2272	4.28
vmtoolsd.exe	1.91	6.1	0.63	127780	2253	7.82
rundll32.exe	2.13	9.8	207.82	289765	2212	0.83
shellexperiencehost.exe	0.84	40.2	0	76078	2265	12.38
searchui.exe	2.87	69.3	0.13	68150	2260	11.89
searchprotocolhost.exe	7.67	11.7	0.28	821404	2141	0.93



Top 15 Applications by Selected Metric

Select a Metric to Graph: Avg CPU (MIPS)



UX Survey

Use Case 16: I would like to augment the data that feeds into the makeup of the User Experience score to count not just objective data from the monitored systemdatapoints and analytics, but also subjective feedback from my end-users about how much they perceive their workday is affected by IT resource constraints.

What do they like or dislike about what our IT team has provisioned for them tobe as effective as possible?

Action: Click on UX Surveys.

To create a survey, refer to Create a Survey.

Results: Provides subjective user feedback on how they feel about their daily work environment which then gets factored into the overall User Experience score for the fleet.

9 Appendix

9.1 Remediation Scripts Help

LDI Plus provides you the following out-of-the-box scripts to get you started.

Script Category	Script Name	Help
Citrix Service Actions	Service_Enable_Citrix_AD_Identity	Enables the Citrix AD Identity Service
Citrix Service Actions	Service_Enable_Citrix_Broker	Enables the Citrix Broker Service
Citrix Service Actions	Service_Enable_Citrix_CDF	Enables the Citrix CDF Service
Citrix Service Actions	Service_Enable_Citrix_Configuration	Enables the Citrix Configuration Service
Citrix Service Actions	Service_Enable_Citrix_Credential_Wallet	Enables the Citrix Credential Wallet Service
Citrix Service Actions	Service_Enable_Citrix_Desktop_Service	Enables the Citrix Desktop Service
Citrix Service Actions	Service_Enable_Citrix_Device_Redirector	Enables the Citrix Device Redirector Service
Citrix Service Actions	Service_Enable_Citrix_Encryption_Service	Enables the Citrix Encryption Service
Citrix Service Actions	Service_Enable_Citrix_EUEM	Enables the Citrix EUEM Service
Citrix Service Actions	Service_Enable_Citrix_Group_Policy_Engine	Enables the Citrix Group Policy Engine Service
Citrix Service Actions	Service_Enable_Citrix_Host	Enables the Citrix Host Service

Citrix Service Actions	Service_Enable_Citrix_Location_and_Sensor_Virtual_Channel	Enables the Citrix Location and Sensor Virtual Channel Service
Citrix Service Actions	Service_Enable_Citrix_Machine_Creation	Enables the Citrix Machine Creation Service
Citrix Service Actions	Service_Enable_Citrix_MultiTouch_Redirection	Enables the Citrix MultiTouch Redirection Service
Citrix Service Actions	Service_Enable_Citrix_Personal_vDisk	Enables the Citrix Personal vDisk Service
Citrix Service Actions	Service_Enable_Citrix_Print_Manager	Enables the Citrix Print Manager Service
Citrix Service Actions	Service_Enable_Citrix_Profile_Management	Enables the Citrix Profile Management Service
Citrix Service Actions	Service_Enable_Citrix_PVS_2StageBoot	Enables the Citrix PVS 2StageBoot Service
Citrix Service Actions	Service_Enable_Citrix_PVS_API	Enables the Citrix PVS API Service
Citrix Service Actions	Service_Enable_Citrix_PVS_BNPXE	Enables the Citrix PVS BNPXE Service
Citrix Service Actions	Service_Enable_Citrix_PVS_BNTFTP	Enables the Citrix PVS BNTFTP Service
Citrix Service Actions	Service_Enable_Citrix_PVS_BOOTP	Enables the Citrix PVS BOOTP Service
Citrix Service Actions	Service_Enable_Citrix_Pvs_for_VMs_Agent	Enables the Citrix Pvs for VMs Agent Service
Citrix Service Actions	Service_Enable_Citrix_PVS_Soap	Enables the Citrix PVS Soap Service
Citrix Service Actions	Service_Enable_Citrix_PVS_Stream	Enables the Citrix PVS Stream Service

Citrix Service Actions	Service_Enable_Citrix_Services_Manager	Enables the Citrix Services Manager Service
Citrix Service Actions	Service_Enable_Citrix_Smart_Card	Enables the Citrix Smart Card Service
Citrix Service Actions	Service_Enable_Citrix_Stack_Control	Enables the Citrix Stack Control Service
Citrix Service Actions	Service_Enable_Citrix_Storefront	Enables the Citrix Storefront Service
Citrix Service Actions	Service_Enable_Citrix_Telemetry	Enables the Citrix Telemetry Service
Citrix Service Actions	Service_Enable_HDX_MediaStream	Enables the Citrix HDX MediaStream Service
Citrix Service Actions	Service_Restart_Citrix_Configuration	Restarts the Citrix Configuration Service
Citrix Service Actions	Service_Restart_Citrix_Credential_Wallet	Restarts the Citrix Credential Wallet Service
Citrix Service Actions	Service_Restart_Citrix_Desktop_Service	Restarts the Citrix Desktop Service
Citrix Service Actions	Service_Restart_Citrix_Device_Redirector	Restarts the Citrix Device Redirector Service
Citrix Service Actions	Service_Restart_Citrix_Encryption_Service	Restarts the Citrix Encryption Service
Citrix Service Actions	Service_Restart_Citrix_EUEM	Restarts the Citrix EUEM Service
Citrix Service Actions	Service_Restart_Citrix_Group_Policy_Engine	Restarts the Citrix Group Policy Engine Service
Citrix Service Actions	Service_Restart_Citrix_Host	Restarts the Citrix Host Service

Citrix Service Actions	Service_Restart_Citrix_Location_and_Sensor_Virtual_Channel	Restarts the Citrix Location and Sensor Virtual Channel Service
Citrix Service Actions	Service_Restart_Citrix_Machine_Creation	Restarts the Citrix Machine Creation Service
Citrix Service Actions	Service_Restart_Citrix_Mobile_Receiver_Virtual_Channel	Restarts the Citrix Mobile Receiver Virtual Channel Service
Citrix Service Actions	Service_Restart_Citrix_MultiTouch_Redirection	Restarts the Citrix MultiTouch Redirection Service
Citrix Service Actions	Service_Restart_Citrix_Personal_vDisk	Restarts the Citrix Personal vDisk Service
Citrix Service Actions	Service_Restart_Citrix_Print_Manager	Restarts the Citrix Print Manager Service
Citrix Service Actions	Service_Restart_Citrix_Profile_Management	Restarts the Citrix Profile Management Service
Citrix Service Actions	Service_Restart_Citrix_PVS_2StageBoot	Restarts the Citrix PVS 2StageBoot Service
Citrix Service Actions	Service_Restart_Citrix_PVS_API	Restarts the Citrix PVS API Service
Citrix Service Actions	Service_Restart_Citrix_PVS_BNPXE	Restarts the Citrix PVS BNPXE Service
Citrix Service Actions	Service_Restart_Citrix_PVS_BNTFTP	Restarts the Citrix PVS BNTFTP Service
Citrix Service Actions	Service_Restart_Citrix_PVS_BOOTP	Restarts the Citrix_PVS_BOOTP Service
Citrix Service Actions	Service_Restart_Citrix_Pvs_for_VMs_Agent	Restarts the Citrix Pvs for VMs Agent Service

Citrix Service Actions	Service_Restart_Citrix_PVS_Soap	Restarts the Citrix PVS Soap Service
Citrix Service Actions	Service_Restart_Citrix_PVS_Stream	Restarts the Citrix PVS Stream Service
Citrix Service Actions	Service_Restart_Citrix_Services_Manager	Restarts the Citrix Services Manager Service
Citrix Service Actions	Service_Restart_Citrix_Smart_Card	Restarts the Citrix Smart Card Service
Citrix Service Actions	Service_Restart_Citrix_Stack_Control	Restarts the Citrix Stack Control Service
Citrix Service Actions	Service_Restart_Citrix_Storefront	Restarts the Citrix Storefront Service
Citrix Service Actions	Service_Restart_Citrix_Telemetry	Restarts the Citrix Telemetry Service
Citrix Service Actions	Service_Restart_HDX_MediaStream	Restarts the Citrix HDX MediaStream Service
Device Configuration Actions	DongleMeteredConnectionSet2Off	This script is used to set DongleOrAny Wireless with meteredconnection property to off
Device Configuration Actions	fixDNSCache	This script will fix the DNS Cache
Device Configuration Actions	GPUpdate-Computer	Runs a computer Group Policy Update with force parameter - run this as the System
Device Configuration Actions	GPUpdate-Full	Runs a full Group Policy Update with force parameter - run this as the System

Device Configuration Actions	GPUpdate-User	Runs a user Group Policy Update with force parameter - run this as the user
Device Configuration Actions	ReRunLogonScript	Finds the location of the user's login script and runs it again if available
Device Configuration Actions	SystemFileCheck	Scans the integrity of all protected system files and repairs files problems when possible - run this as system
Microsoft Office Actions	ClearCachedOfficeCredentials	Clears the cached credentials for Office using the cmdkey command and matching credentials with MicrosoftOffice16_Data in the name - run this as the User
Microsoft Office Actions	ClearSkypeCachePassword	Removes skype cached password
Microsoft Office Actions	ClearSkypeforBusinessCache	Clears the Skype for Business Cache - run as the user
Microsoft Office Actions	DisableOutlookAutoComplete	Disables outlook auto complete
Microsoft Office Actions	Enable_OutlookSearch	Enables outlook search
Microsoft Office Actions	Excel_Enable_All_Macros	Changes the users registry value to enable all macros in Excel updates HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Security:vbawarnings for the user - run this as the user

Microsoft Office Actions	Excel_Enable_Developer_Tools	Changes the users registry value to enable the developer tools in Excel updates HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Options - DeveloperTools for the user - run this as the user
Microsoft Office Actions	Excel_Enable_Signed_Macros	Changes the users registry value to enable signed macros in Excel updates HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Security:vbawarnings for the user - run this as the user
Microsoft Office Actions	Office16ClearDocCache	Clears the Office 16 Document cache - run as the user
Microsoft Office Actions	Office16SetClearDocCacheOnExit	Sets the Office 16 Document cache to be cleared on document closure - runs as the user
Microsoft Office Actions	OneDriveReset	Resets Microsoft OneDrive this can sometimes resolve sync issues and resets all OneDrive settings. OneDrive performs a full sync after the reset. You won't lose any data by resetting OneDrive. - runs this as the user
Microsoft Office Actions	OST_RemoveUserProfileGT60	Removes 60 days old ost file from profile
Microsoft Office Actions	OST_RepairRemoveRestartOutlook	Removes problemOrtroubled ost file and restart the outlook

Microsoft Office Actions	PowerPoint_Enable_All_Macros	Changes the users registry value to enable all macros in PowerPoint updates HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\PowerPoint\Security:vbawarnings for the user - run this as the user
Microsoft Office Actions	PowerPoint_Enable_Developer_Tools	Changes the users registry value to enable the developer tools in PowerPoint updates HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\PowerPoint\Options - DeveloperTools for the user - run this as the user
Microsoft Office Actions	PowerPoint_Enable_Signed_Macros	Changes the users registry value to enable signed macros in PowerPoint updates HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\PowerPoint\Security:vbawarnings for the user - run this as the user
Microsoft Office Actions	WindowsDefenderFullScan	Runs a Windows Defender Full Scan
Microsoft Office Actions	WindowsDefenderQuickScan	Runs a Windows Defender Quick Scan
Microsoft Office Actions	WindowsDefenderUpdateDefinitions	Updates the Windows Defender Signatures - this can be useful in troubleshooting - run as the System
Microsoft Office Actions	WindowsHardwareDiagnostic	Runs the Windows Hardware Diagnostic wizard - run this as the user
Microsoft Office Actions	WindowsInternetDiagnostic	Runs the Windows Internet Diagnostic wizard - run this as the user

Microsoft Office Actions	WindowsNetworkDiagnostic	Runs the Windows Network Diagnostic wizard - run this as the user
Microsoft Office Actions	WindowsPrinterDiagnostic	Runs the Windows Printer Diagnostic wizard - run this as the user
Microsoft Office Actions	WindowsUpdateDiagnostic	Runs the Windows Update Diagnostic wizard - run this as the user
Microsoft Office Actions	WindowsUpdateResetDownloadFolders	Stops the Windows update services and renames the download folders then restarts the services - run this as the system
Microsoft Office Actions	Word_Enable_All_Macros	Changes the users registry value to enable all macros in Word updates HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Security:vbawarnings for the user - run this as the user
Microsoft Office Actions	Word_Enable_Developer_Tools	Changes the users registry value to enable the developer tools in Word updates HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Options - DeveloperTools for the user. This action needs to be run this as the user.
Microsoft Office Actions	Word_Enable_Signed_Macros	Changes the users registry value to enable signed macros in Word updates HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Security:vbawarnings for the user. This action needs to be run this as the user.
Microsoft SCCM Actions	SCCM-Agent-repair	Runs the SCCM Agent repair program.

Microsoft SCCM Actions	SCCM-Agent-restart	Runs the SCCM Agent restart program.
Microsoft SCCM Actions	SCCM-ClearCache	Clears the SCCM Agent cache by default this is the directory %windir%\ccmcache
Microsoft SCCM Actions	SCCM-Client-AppDeployEvalCycle	Trigger an SCCM Client Application Deployment Evaluation Cycle - run this as system
Microsoft SCCM Actions	SCCM-Client-DiscoveryDataCollectionCycle	Triggers an SCCM Client Discovery Data Collection Cycle - run this as system
Microsoft SCCM Actions	SCCM-Client-FileCollectionCycle	Triggers an SCCM Client File Collection Cycle - run this as system
Microsoft SCCM Actions	SCCM-Client-HardwareInventoryCycle	Triggers an SCCM Hardware Inventory Cycle - run this as system
Microsoft SCCM Actions	SCCM-Client-MachinePolicyEvaluationCycle	Triggers an SCCM Machine Policy Evaluation Cycle - run this as system
Microsoft SCCM Actions	SCCM-Client-MachinePolicyRetrievalCycle	Triggers an SCCM Machine Policy Retrieval Cycle - run this as system
Microsoft SCCM Actions	SCCM-Client-SftwrMeteringRptCycle	Triggers an SCCM Software Metering Usage Report Cycle - run this as system
Microsoft SCCM Actions	SCCM-Client-SftwrUpdateAssgnmtEval	Triggers an SCCM Software Updates Assignments Evaluation Cycle - run this as system
Microsoft SCCM Actions	SCCM-Client-SoftwareInventoryCycle	Triggers an SCCM Software Inventory Cycle - run this as system

Microsoft SCCM Actions	SCCM-Client-SoftwareUpdateScanCycle	Triggers an SCCM Software Update Scan Cycle - run this as system
Microsoft SCCM Actions	SCCM-Client-StateMessageRefresh	Triggers an SCCM State Message Refresh - run this as system
Microsoft SCCM Actions	SCCM-Client-UserPolicyEvaluationCycle	Triggers an SCCM User Policy Evaluation Cycle - run this as system
Microsoft SCCM Actions	SCCM-Client-UserPolicyRetrievalCycle	Triggers an SCCM User Policy Retrieval Cycle - run this as system
Microsoft SCCM Actions	SCCM-Client-WindowsSrcListUpdate	Triggers an SCCM Windows Installers Source List Update Cycle - run this as system
Microsoft SCCM Actions	SCCM-Set-Site	Changes the local machine registry value to update the SCCM site updates HKLM\SOFTWARE\Microsoft\CCM\CcmEval:LastSiteCode HKLM\SOFTWARE\Microsoft\SMS\DP:SiteCode and HKLM\SOFTWARE\Microsoft\SMS\Mobile Client:AssignedSiteCode
Remote Sessions Actions	Service_Enable_HDX_MediaStream	Enables the Citrix HDX MediaStream Service
Remote Sessions Actions	Service_Restart_HDX_MediaStream	Restarts the Citrix HDX MediaStream Service
Remote Work Actions	Service_Enable_Zoom_Sharing	Enables the Zoom Sharing Service
Remote Work Actions	Service_Restart_Zoom_Sharing	Restarts the Zoom Sharing Service
Security Actions	Service_Enable_1EClient	Enables the 1E Client Service

Security Actions	Service_Enable_Bitlocker	Enables the Bitlocker Service
Security Actions	Service_Enable_Cisco_acumbrella	Enables the Cisco acumbrellaagent Service
Security Actions	Service_Enable_Cisco_Umbrella	Enables the Cisco Umbrella_RC Service
Security Actions	Service_Enable_ClearPass_Agent	Enables the ClearPass Agent Controller Service
Security Actions	Service_Enable_ClearPass_OnGuard	Enables the ClearPass OnGuard Agent Service
Security Actions	Service_Enable_CrowdStrikeFalcon	Enables the CrowdStrike Falcon Service
Security Actions	Service_Enable_DefenderATP	Enables the Windows Defender ATP Service
Security Actions	Service_Enable_Defender_Firewall	Enables the Windows Defender Firewall Service
Security Actions	Service_Enable_Defender_NIS	Enables the Windows Defender Antivirus Network Inspection Service
Security Actions	Service_Enable_FortiClient_VPN	Enables the Fortinet SslvpnDaemon Service
Security Actions	Service_Enable_iDAppsService	Enables the iDAppsService Service
Security Actions	Service_Enable_McAfeeFramework	Enables the McAfee Agent Backwards Compatibility Service
Security Actions	Service_Enable_McAfee_AgentService	Enables the McAfee Agent Service
Security Actions	Service_Enable_McAfee_macmnsvc	Enables the McAfee Agent Common Services Service

Security Actions	Service_Enable_NomadBranch	Enables the NomadBranch Service
Security Actions	Service_Enable_Symantec_Broker	Enables the Symantec Privilege Broker Service
Security Actions	Service_Enable_Symantec_EP	Enables the Symantec Endpoint Protection Service
Security Actions	Service_Enable_Symantec_EPLP	Enables the Symantec Endpoint Protection Local Proxy Service
Security Actions	Service_Enable_Symantec_EPWSC	Enables the Symantec Endpoint Protection WSC Service
Security Actions	Service_Enable_Symantec_IDS	Enables the Symantec IDS Service
Security Actions	Service_Enable_Symantec_IPS	Enables the Symantec IPS Service
Security Actions	Service_Enable_Symantec_Util	Enables the Symantec Util Service
Security Actions	Service_Enable_Tanium_Client	Enables the Tanium Client Service
Security Actions	Service_Enable_Trend_CCSF	Enables the Trend Micro Common Client Solution Framework Service
Security Actions	Service_Enable_Trend_Firewall	Enables the Trend Micro Security Agent Firewall Service
Security Actions	Service_Enable_Trend_Listener	Enables the Trend Micro Security Agent Listener Service
Security Actions	Service_Enable_Trend_NTRTScan	Enables the Trend Micro Security Agent Real-time Scan Service

Security Actions	Service_Enable_Trend_TMBM	Enables the Trend Micro Unauthorized Change Prevention Service
Security Actions	Service_Restart_1EClient	Restarts the 1E Client Service
Security Actions	Service_Restart_Bitlocker	Restarts the Bitlocker Service
Security Actions	Service_Restart_Cisco_acumbrella	Restarts the Cisco acumbrellaagent Service
Security Actions	Service_Restart_Cisco_Umbrella	Restarts the Cisco Umbrella_RC Service
Security Actions	Service_Restart_ClearPass_Agent	Restarts the ClearPass Agent Controller Service
Security Actions	Service_Restart_ClearPass_OnGuard	Restarts the ClearPass OnGuard Agent Service
Security Actions	Service_Restart_CrowdStrikeFalcon	Restarts the CrowdStrike Falcon Service
Security Actions	Service_Restart_DefenderATP	Restarts the Windows Defender ATP Service
Security Actions	Service_Restart_Defender_Firewall	Restarts the Windows Defender Firewall Service
Security Actions	Service_Restart_Defender_NIS	Restarts the Windows Defender Antivirus Network Inspection Service
Security Actions	Service_Restart_iDAppsService	Restarts the iDAppsService Service
Security Actions	Service_Restart_McAfeeFramework	Restarts the McAfee Agent Backwards Compatibility Service
Security Actions	Service_Restart_McAfee_AgentService	Restarts the McAfee Agent Service

Security Actions	Service_Restart_McAfee_macmnsvc	Restarts the McAfee Agent Common Services Service
Security Actions	Service_Restart_NomadBranch	Restarts the NomadBranch Service
Security Actions	Service_Restart_Symantec_Broker	Restarts the Symantec Privilege Broker Service
Security Actions	Service_Restart_Symantec_EP	Restarts the Symantec Endpoint Protection Service
Security Actions	Service_Restart_Symantec_EPLP	Restarts the Symantec Endpoint Protection Local Proxy Service
Security Actions	Service_Restart_Symantec_EPWSC	Restarts the Symantec Endpoint Protection WSC Service
Security Actions	Service_Restart_Symantec_IDS	Restarts the Symantec IDS Service
Security Actions	Service_Restart_Symantec_IPS	Restarts the Symantec IPS Service
Security Actions	Service_Restart_Symantec_Util	Restarts the Symantec Util Service
Security Actions	Service_Restart_Tanium_Client	Restarts the Tanium Client Service
Security Actions	Service_Restart_Trend_CCSF	Restarts the Trend Micro Common Client Solution Framework Service
Security Actions	Service_Restart_Trend_Firewall	Restarts the Trend Micro Security Agent Firewall Service
Security Actions	Service_Restart_Trend_Listener	Restarts the Trend Micro Security Agent Listener Service

Security Actions	Service_Restart_Trend_NTRTScan	Restarts the Trend Micro Security Agent Real-time Scan Service
Security Actions	Service_Restart_Trend_TMBM	Restarts the Trend Micro Unauthorized Change Prevention Service
Sensor Actions	Disk Cleanup	Cleans the C: drive's Window Temporary Internet Files for all users and empties the recycling bin.
Sensor Actions	Rebuild WMI	Goes through the recommended WMI rebuild actions as described by Microsoft. If no parameter is passed, the script defaults to its Alarm only setting and a log is generated in the location the script is run. Note: This script restarts the WMI service as part of its operation. This results in a service that depends on WMI restarting which as well can result in problems such as VDI session disconnects.
Sensor Actions	Restart Base Filtering Service	Restarts the Base Filtering Service, which is responsible for managing firewall and IPsec policies and user mode filtering.
Sensor Actions	Restart Computer	Restarts the computer.
Sensor Actions	Restart Cryptographic Service	Restarts the Cryptographic Service which controls the certificates that are trusted as well as confirming the signatures of Windows files.
Sensor Actions	Restart DCOM Service	Restarts the DCOM Service which controls the launch of COM and DCOM servers in response to object activation requests.

Sensor Actions	Restart DHCP Service	Restarts the DHCP Service which registers and updates IP addresses and DNS records for the computer.
Sensor Actions	Restart DNS Client Service	Restarts the DNS Client Service which cache DNS names and registers the full name for the computer.
Sensor Actions	Restart Event Broker Service	Restarts the Event Broker Service which coordinates the execution of background work for WinRT applications.
Sensor Actions	Restart LAN Manager Service	Restarts the LAN Manager Service which creates and maintains connections to remote servers.
Sensor Actions	Restart Local Session Manager Service	Restarts the Local Session Manager Service which manages local user sessions.
Sensor Actions	Restart Netlogon Service	Restarts the Netlogon Service which maintains a secure channel to the domain controller for authentication.
Sensor Actions	Restart NIC	Restarts the Network Adapters on the system.
Sensor Actions	Restart NLA Service	Restarts the NLA Service which collects and stores configuration information for the network.
Sensor Actions	Restart Plug and Play Service	Restarts the Plug and Play Service which enables the computer to recognize and adapt to hardware changes.

Sensor Actions	Restart Printer Spooler Service	Restarts the Printer Spooler Service which spools print jobs and handles interactions with the printer.
Sensor Actions	Restart RPC Service	Restarts the RPC Service which performs object activations object exporter resolutions and garbage collection for the COM and DCOM servers.
Sensor Actions	Restart Server Service	Restarts the Server Service which supports file print and named-pipe sharing over the network.
Sensor Actions	Restart Task Scheduler Service	Restarts the Task Scheduler Service which enables the configuration and scheduling of automated tasks.
Sensor Actions	Restart Time Broker Service	Restarts the Time Broker Service which coordinates background work for WinRT applications.
Sensor Actions	Restart User Profile Service	Restarts the User Profile Service which is responsible for loading and unloading user profiles.
Sensor Actions	Restart Windows Defender Service	Restarts the Windows Defender Service which helps protect the computer from unauthorized access.
Sensor Actions	Restart Windows Event Log Service	Restarts the Windows Event Log Service which manages events and event logs.
Sensor Actions	Restart Windows Update Service	Restarts the Windows Update Service which controls the download and install of Windows Updates.
Sensor Actions	Start Windows Firewall	Starts the Windows Firewall.

VPN Actions	Service_Enable_CiscoAnyConnect	Enables the Cisco AnyConnect VPN Service
VPN Actions	Service_Enable_ClearPass_VPN	Enables the ClearPass VPN Service
VPN Actions	Service_Enable_Juniper_NetConnect	Enables the Juniper NETConnect Service
VPN Actions	Service_Enable_Zscaler	Enables the ZSAService Service
VPN Actions	Service_Enable_Zscaler_Tunnel	Enables the ZSATunnel Service
VPN Actions	Service_Restart_FortiClient_VPN	Restarts the Fortinet SslvpnDaemon Service
VPN Actions	Service_Restart_Juniper_NetConnect	Restarts the Juniper NETConnect Service
VPN Actions	Service_Restart_Zscaler	Restarts the ZScaler Service
VPN Actions	Service_Restart_Zscaler_Tunnel	Restarts the ZSATunnel Service

9.2 Device Support Matrix

9.2.1 LDI Plus OEM and OS Support Matrix

Module	**Sub-Module**	**Sub Module Menu**	**Operating System**		**Win VM**		**Manufacturer**				
			Win10 & 11	**macOS**			**Agnostic**	**Lenovo**	**HP**	**Dell**	**MS Surface**
Issues & Reports	BSOD Crashes		X					X	X		X
	AppPerformance		X				X				
	Batteries		X					X			
	Storage Drives		X					X	*NVMe	*NVMe	*NVMe
	Available Updates		X					X			
	Additional Reports		X				X				
User Experience	Fleet Overview	Application Faults	X	X	X		X				
		Application Virtualization	X		X		X				
		Applications	X	X	X		X				

		Software Packages	X	X	X		X				
		Analysis	X	X	X		X				
	Device Overview	Application Faults	X	X	X		X				
		Application Latency	X	X	X		X				
		Application Virtualization	X		X		X				
		Applications	X	X	X		X				
		Boot and Login	X		*env. dep.		X				
		Computer Concerns	X	X	X		X				
		Computer Performance	X	X	X		X				
		Hardware	X	X	X		X				
		Health	X		X		X				
		Power	X	X	*env. dep.		X				

		Software Packages	X	X	X		X				
		Storage	X	X	*env. dep.		X				
		System Mobility	X	X	X		X				
	Risk Analysis	Application Security	X	X	X		X				
		Security Risk	X		X		X				
		Systems with Risk Applications	X	X	X		X				
		User Security	X	X	X		X				
	Persona Summary	Persona Critical Applications	X	X	X		X				
		User Critical Applications	X	X	X		X				
		User Details	X	X	X		X				

		User Resource Consumption	X	X	X		X				
		User Systems	X	X	X		X				
	Sector Benchmarks		X		X		X				
UX Surveys	Create a Survey		X		X		X				
	Send Survey *tray app		X		X		X				
	Survey Results		X		X		X				
Discover & Resolve	Like Dashboards and Analytic tabs, this is a cloud toolset that uses the available data that has been collected for each system.										
Device Lookup	Black Box		X	X	X		X				
	Health		X	X	X		X				
	System Usage		X	X	X		X				
	Dependencies		X	X	X		X				
	Hardware		X	X	X		X				
	Hardware Diagram		X	X	X		X				
	Software		X	X	X		X				
	Faults		X	X	X		X				
	Web Performance		X	X	X		X				
	*has temp limitations										
	Boot/Logon Time		X		X		X				
	Logon Process		X		X		X				

	Event Correlation	X	X	X		X				
	All Inventory	X								
	Graphing	X	X	X		X				
	Comparative Analysis	X	X	X		X				
	File Information	X	X	X		X				
	Power Schedule	X		*env. dep.		X				
	Tools	Notify and prompt mode will require tray app running, no tray app currently for macOS.								
App Vision	Modules	X	X	X		X				
	Connections	X	X	X		X				
	Network Graphing	X	X	*env. dep.		X				
	Virtualization	Insights into application virtualization difficulty, not currently supported.								
	Faults	X	X	X		X				
	CPU	X	X	X		X				
	Memory	X	X	X		X				
	I/O	X	X	*env. dep.		X				
	Network	X	X	*env. dep.		X				
	Times	X	X	X		X				
	GPU	X	X	X		X				
	Systems	X	X	*env. dep.		X				
Device Manager	Devices	X	X	X		X				

Configuration	Insights & Automations	Automations	X	X	X		X				
		Role Management	X	X	X		X				
		Policies	X	X	X		X				
	*tray app	System Assignments	X	X	X		X				
		Alarm Notifications	X	X	X		X				
		Alarm Actions	X	X	X		X				
		Administration	X	X	X		X				
	Sensor Configuration *sensors		X	X	X		X				

9.2.1.1. Additional Notes

*env. dep. → Environmental Dependency, most commonly applicable to Virtual Machines where there are various possible configurations that may introduce limitations such as non-persistent storage mediums.

*tray app → When using automations, notify and prompt mode require the LsiClientTrayApp.exe in <C:\Program Files (x86)\SysTrack\LsiAgent\Utilities> to be running, and is not supported in macOS (automations ran in silent mode will work in macOS).

*sensors → Sensor Analysis functions on all platforms and Sensor Actions are platform-specific based on the Actions' configurations.

*NVMe → Primarily NVMe drive variant support, please reach out for more information if needed.